PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-208515
(43)Date of publication of application : 26.07.1994

(51)Int.Cl. G06F 12/14

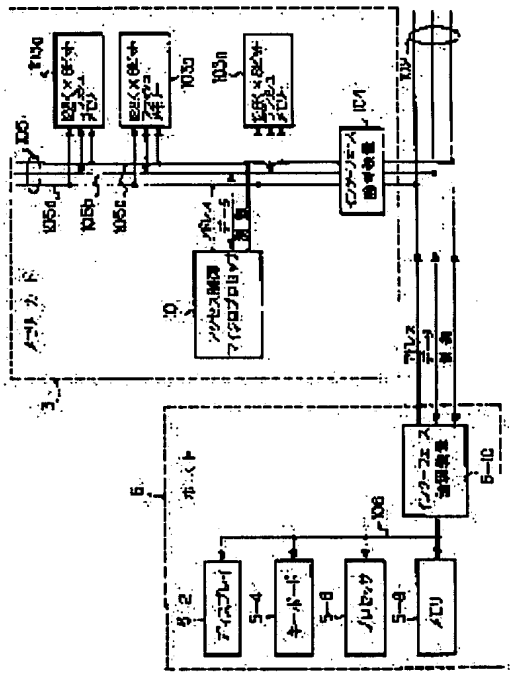
(21)Application number : 05-256786
(22)Date of filing : 14.10.1993

(71)Applicant : BULL HN INF SYST INC
(72)Inventor : HOLTEY THOMAS O
WILSON PETER J

(30)Priority
Priority number : 92 960748 Priority date : 14.10.1992 Priority country : US

(54) MEMORY CARD

(57)Abstract:
PURPOSE: To provide a security memory card containing a microprocessor on one semiconductor chip and one or more nonvolatile addressable memory chips.
CONSTITUTION: Both a microprocessor chip and a nonvolatile memory chip are connected to an internal card bus and addresses, data, and control information are transferred to the nonvolatile memory chip. A microprocessor 5-6 stores information containing many key values, configuration information peculiar to the use, and program instruction information. The memory of each chip is constituted in many blocks, namely, banks and each memory chip is constituted to contain a security control logic circuit. The circuits contain pluralities of nonvolatile and volatile storage devices which are loaded with keys and configuration information under the control of the microprocessor 5-6 only after the microprocessor 5-6 discriminates that a user successfully performs confirming procedures predecided by a host computer 5. Thereafter, the user is allow to read out information only from such a block as that defined by the configuration information.



LEGAL STATUS

[Date of request for examination]	29.06.1999
[Date of sending the examiner's decision of rejection]	08.04.2003
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3493047
[Date of registration]	14.11.2003

[Number of appeal against examiner's decision of rejection]	2003-012861
[Date of requesting appeal against examiner's decision of rejection]	07.07.2003
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平6－208515

(43)公開日　平成６年(1994)７月26日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　12/14	３２０　Ａ	9293－5B		

審査請求　未請求　請求項の数26　ＯＬ　（全 19 頁）

(21)出願番号　特願平5－256786

(22)出願日　平成５年(1993)10月14日

(31)優先権主張番号　９６０７４８

(32)優先日　1992年10月14日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　391031270
ブル・エイチエヌ・インフォメーション・システムズ・インコーポレーテッド
BULL HN INFORMATION SYSTEMS, INCORPORATED
アメリカ合衆国マサチューセッツ州01821，ビレリカ，テクノロジー・パーク（番地なし）

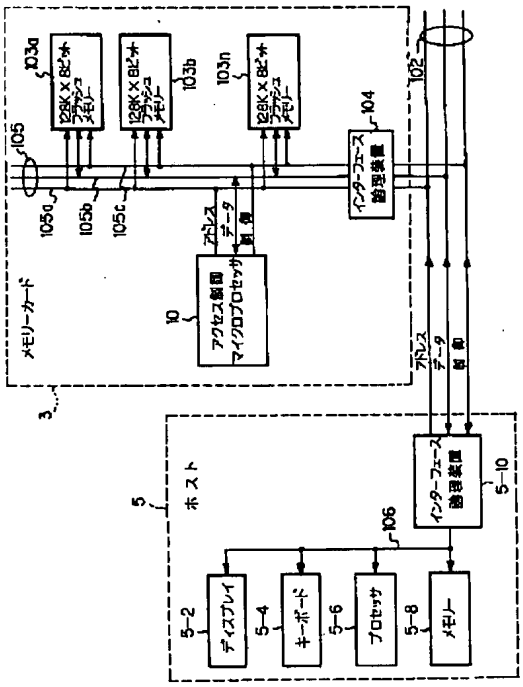
(72)発明者　トーマス・オー・ホルティー
アメリカ合衆国マサチューセッツ州02162，ニュートン，クレホアー・ドライブ　10

(74)代理人　弁理士　湯浅　恭三　（外５名）

最終頁に続く

(54)【発明の名称】　メモリー・カード

(57)【要約】
【目的】１つの半導体チップ上のマイクロプロセッサと、１つ以上の不揮発性のアドレス指定可能なメモリー・チップとを含む機密保護メモリー・カードを提供する。
【構成】マイクロプロセッサ・チップと不揮発性メモリー・チップとは、共に内部カード・バスに接続して、アドレスとデータと制御情報とを前記不揮発性メモリー・チップへ転送する。マイクロプロセッサは、多数のキー値を含む情報と、用途に固有の構成情報と、プログラム命令情報とを含む。各チップのメモリーは、多数のブロック即ちバンクに構成され、各メモリー・チップは機密保護制御論理回路を含むように構成される。これらの回路は、ユーザがホスト・コンピュータによる予め定めた確認手順を成功裏に実施したことをマイクロプロセッサが判定した後にのみ、マイクロプロセッサの制御下でキーおよび構成情報でロードされる複数の不揮発性および揮発性の記憶装置を含んでいる。その後、ユーザは、構成情報により定義される如きブロックのみからの情報の読出しを許容される。



1

【特許請求の範囲】

【請求項１】　ホストの携帯コンピュータと共に使用される機密保護メモリー・カードにおいて、

前記ホスト・コンピュータに対しおよびこれからアドレス、データおよび制御情報を送受するように接続されたマイクロプロセッサを設け、該マイクロプロセッサは、複数のキー値を含む情報と構成情報とを記憶するアドレス指定可能不揮発性メモリーを含み、

前記マイクロプロセッサに接続されて、アドレスとデータと前記カードにより行われるべきメモリー動作を定義する制御情報とを伝送する内部バスと、

前記マイクロプロセッサと共通に前記内部バスに接続されて、前記アドレスとデータと制御情報とを受取る少なくとも１つの不揮発性のアドレス指定可能メモリーとを設け、前記メモリーは、不揮発性記憶セクションと機密保護制御セクションとを含み、該記憶セクションは複数のブロックに構成されたメモリー・アレイを含み、各ブロックは複数のアドレス指定可能な場所と前記記憶動作を行う制御論理手段とを有し、前記機密保護制御セクションは前記内部バスと前記制御論理手段と前記メモリー・アレイとに接続され、前記機密保護制御セクションは、

前記ブロックと関連する少なくとも一つの前記キー値と構成情報を記憶する複数の不揮発性および揮発性記憶装置と、

前記制御論理手段と前記記憶装置とに接続されたアクセス制御論理手段とを含み、該アクセス制御論理手段は、前記マイクロプロセッサが予め定めた確認手順が前記ホスト・コンピュータにより行われて前記アクセス制御論理手段が前記構成情報に従って前記メモリー・アレイからの前記情報の読出しを許容することを可能にしたと判定した後のみ、前記構成情報により指定される如き前記メモリー・アレイの前記ブロックのアドレス指定されたものに記憶された情報の読出しを可能にすることを特徴とするメモリー・カード。

【請求項２】　前記マイクロプロセッサおよび前記不揮発性メモリーが個々の半導体チップ上に含まれることを特徴とする請求項１記載のメモリー・カード。

【請求項３】　前記カードが更に、該カードを前記ホスト・コンピュータに接続するインターフェース回路手段を含み、該インターフェース回路手段および前記マイクロプロセッサが同じ半導体チップ上に含まれることを特徴とする請求項１記載のメモリー・カード。

【請求項４】　前記不揮発性メモリー・カードおよび前記不揮発性記憶装置がフラッシュ・メモリーであることを特徴とする請求項１記載のメモリー・カード。

【請求項５】　前記不揮発性記憶装置の一方が、前記１つのキー値と対応するロック値を記憶するロック・メモリーであり、前記不揮発性装置の第２のものが前記ロック・メモリーに接続するロック記憶可能化要素であり、

2

前記ロック・メモリーが最初に前記ロック値でロードされ、前記ロック記憶可能化要素が、前記マイクロプロセッサの制御下で前記ロック値の修正を禁止する状態へ切換えられることを特徴とする請求項１記載のメモリー・カード。

【請求項６】　前記ロック値の記憶および前記ロック記憶可能化要素の切換えが、前記メモリー・カードの初期の製造中に起生することを特徴とする請求項２記載のメモリー・カード。

【請求項７】　前記揮発性記憶装置の一方が、数において前記構成情報を記憶するための前記メモリー・アレイのブロック数と対応する複数の記憶域を持つアドレス指定可能なアクセス制御メモリーであり、該アクセス制御メモリーが前記内部バスと前記アクセス制御論理手段とに接続され、前記予め定めた確認手順が、前記アクセス制御論理手段による前記アクセス制御メモリーの可能化を生じる前記ホスト・コンピュータにより最初に成功裏に行われたことを判定した後にのみ、前記アクセス制御メモリーが前記マイクロプロセッサの制御下でロードされることを特徴とする請求項５記載のメモリー・カード。

【請求項８】　前記ロック・メモリーにロードされた前記ロック値が全て１であり、前記機密保護制御セクションが更に、前記ロック・メモリーに接続された全て１の検出回路を含み、該検出回路が前記全て１のロック値に応答して、前記機密保護制御セクションを有効にバイパスする信号を生成して、前記不揮発性メモリーがあたかも前記機密保護制御セクションが含まれなかったかのように動作することを可能にすることを特徴とする請求項７記載のメモリー・カード。

【請求項９】　前記予め定めた確認手順の実施が、前記メモリー・カードが前記ホスト・コンピュータと通信するように最初に接続される時に初めて起生することを特徴とする請求項７記載のメモリー・カード。

【請求項１０】　前記アクセス制御メモリーが、前記ロック・メモリーから前記ロック値を受取るように接続されたロック・レジスタと、コンパレータ回路と、前記マイクロプロセッサにより前記キー・レジスタに送られるキー値を記憶するキー・レジスタと、予め定めた時間間隔を定義するカウントを記憶する遅延カウンタと、前記アクセス制御メモリーと前記コンパレータと前記遅延カウンタとに接続されたゲート手段とを含み、前記コンパレータ回路が、前記ロックおよびキー・レジスタと前記ゲート手段とに接続され、該ゲート手段が前記遅延カウンタに接続されて、前記遅延カウンタが前記予め定めた時間間隔の終りを信号した時前記ロック・レジスタにロードされる前記ロック・コード値間の同じ比較を信号する前記コンパレータ回路に応答してアクセス修正許容信号を生じ、前記アクセス修正許容信号が前記構成情報をロードするように前記アクセス制御メモリーを条件付け

る信号を許容することを特徴とする請求項９記載のメモリー・カード。

【請求項１１】　前記制御論理手段が、各メモリー・チップの前記機密保護制御セクションの動作を制御する際に前記マイクロプロセッサにより使用される予め定めた指令セットに応答して指令信号を生じる回路を含むことを特徴とする請求項１０記載のメモリー・カード。

【請求項１２】　前記制御論理手段が、前記マイクロプロセッサにより生じる前記予め定めた指令セットの最初のものに応答して、前記ロック・コード値を前記ロック・メモリーにロードする第１の信号を生じ、該予め定めた指令の前記最初のものが前記カードの初期の製造中に生成されることを特徴とする請求項１１記載のメモリー・カード。

【請求項１３】　前記制御論理手段が、前記マイクロプロセッサにより生成された前記予め定めた指令セットの第２のものに応答して、前記ロック記憶可能化要素を、前記ロック・メモリーに記憶された前記ロック値に対する前記読出しまたは修正を禁止する予め定めた状態へ切換えるための第２の信号を生じることを特徴とする請求項１２記載のメモリー・カード。

【請求項１４】　前記制御論理手段が、前記マイクロプロセッサにより生じた前記予め定めた指令セットの第３のものに応答して、前記キー値の予め定めたもので前記予め定めたキー・レジスタをロードする第３の信号を生じ、前記予め定めた指令セットの前記第３のものが、前記予め定めた確認手順が成功裏に行われたことを前記マイクロプロセッサが判定した後にのみ、前記マイクロプロセッサにより生じることを特徴とする請求項１２記載のメモリー・カード。

【請求項１５】　前記制御論理手段により生じる前記第３の信号が、前記遅延カウンタを前記予め定めた時間間隔の開始を確立する予め定めたカウントに同時に強制し、前記制御論理手段が、前記マイクロプロセッサにより生じる前記予め定めた指令セットの第４のものの各々に応答して前記予め定めたカウントを１だけ減分し、前記遅延カウンタが、前記予め定めた指令セットの予め定めた数の前記第４のものの実行に続く前記時間間隔の前記終りを信号することを特徴とする請求項１４記載のメモリー・カード。

【請求項１６】　前記予め定めた制御論理手段が、前記マイクロプロセッサによる前記予め定めた指令セットの第５および第６の複数に応答して、情報の読出しが許容される前記ブロックのどれかを判定するため前記構成情報に従って前記アクセス制御メモリーにおける場所をセットしリセットするための第５および第６の信号を生じることを特徴とする請求項１１記載のメモリー・カード。

【請求項１７】　前記ホスト・コンピュータとの通信を確立するためホストの携帯コンピュータに組込み可能な

機密保護メモリー・カードにおいて、

単一の半導体チップ上に含まれるマイクロプロセッサを設け、該マイクロプロセッサは、前記ホスト・コンピュータに対しかつこれからアドレスとデータと制御情報とを送受するよう接続され、該マイクロプロセッサは、

記憶域に対するユーザのアクセス可能性を定義する複数のキー値を含む情報と、前記記憶域に対するメモリー読出しアクセス可能性を定義するメモリー構成情報とを記憶するためのアドレス指定可能な不揮発性メモリーを含み、

アドレスとデータと前記カードにより行われるべき記憶動作を定義する制御情報とを伝送する内部バスと、

前記アドレスとデータと制御情報とを受取るため前記マイクロプロセッサと共通に前記内部バスに接続された少なくとも１つの不揮発性のアドレス指定可能なメモリー・チップとを設け、該メモリー・チップは１つの記憶セクションと１つの機密保護セクションとを含み、該記憶セクションはデータ出力を有する不揮発性のメモリー・アレイを含んで各々が複数のアドレス指定可能な場所を有する複数のブロックに構成され、前記記憶動作を行うための制御論理手段を含み、前記機密保護セクションは、前記内部バスと前記制御論理手段と前記データ出力とに接続され、該機密保護セクションは、

前記内部バスに接続されて前記キー値数の１つと合致する予め定めたロック値を最初に受取りかつこれを恒久的に記憶する不揮発性ロック・メモリーと、

前記制御論理手段および前記ロック・メモリーと接続されて、前記予め定めたロック・コード値が前記マイクロプロセッサにより前記内部バスに与えられた前記キー値の選択された１つに識別可能に合致する時を検出すると同時に、可能化信号を生じるアクセス制御論理手段と、

前記読出し可能性を定義する前記記憶構成情報を記憶するための数において前記メモリー・アレイの前記ブロック数と対応する複数の場所を有するアドレス指定可能な揮発性アクセス制御メモリーとを含み、前記アクセス制御メモリーが、前記制御論理手段と前記メモリー・アレイのデータ出力と前記内部バスと前記アクセス制御論理手段とに接続され、該アクセス制御論理手段は、予め定めた確認手順が前記ホスト・コンピュータにより成功裏に行われ、かつ前記記憶のキー・コードの前記予め定めた１つを転送して、前記アクセス制御メモリーの構成情報により指定される如き前記データ出力に加えるための前記可能化信号を、前記アクセス制御論理手段をして前記データ出力に加えられる前記可能化信号を生じさせたことを前記マイクロプロセッサが判定した後にのみ、前記記憶構成情報により指定される如き前記メモリー・アレイの読出しを可能にすることを特徴とするメモリー・カード。

【請求項１８】　各々が複数のモードにおける動作能力を有するアドレス指定可能な場所のブロックに構成され

たメモリー・アレイを含む複数の不揮発性メモリー・チップを含む機密保護メモリー・カードにおいて、
ロック値を記憶するロック・メモリーと、
第1および第2の指令と予め定めたキー値とを生成する制御手段と、
前記制御手段に接続されて、前記第1の指令に応答して前記予め定めたキー値を記憶するキー・レジスタと、
前記ロック・メモリーおよび前記キー・レジスタに接続され、前記ロック値および前記予め定めたキー値が等しい時は常に比較信号を生成するコンパレータと、
前記生成手段に接続され、かつ前記第1の指令に応答して前記カウンタを最大カウント値に設定し、かつ一連の連続する第2の指令に応答して前記遅延カウンタがゼロに減分された時ゼロ・カウント信号を生じる遅延カウンタと、
前記コンパレータおよび前記遅延カウンタに接続され、前記比較信号および前記ゼロ・カウント信号に応答してアクセス修正許容信号を生じる論理回路手段とを設け、
前記制御手段が、第3の指令と、前記第1のブロックおよび以降のブロックをそれぞれ識別する第1のアドレス信号と以降のアドレス信号とを生じ、
前記論理手段と前記制御手段とに接続されたアクセス制御メモリー手段を設け、該アクセス制御メモリーは、前記アクセス記憶可能化信号と前記アドレス信号と前記第3の指令とに応答して、前記ブロックおよび前記以降のブロックの内の一つが読出しのため可能状態にされる時を指定する表示を記憶することを特徴とするメモリー・カード。

【請求項19】　前記メモリー・カードが不当なホスト・コンピュータに配置される時、前記予め定めた値および最大値が、前記不揮発性メモリーに記憶された前記情報に対する容易なアクセスを阻止するように充分に大きく選定されることを特徴とする請求項18記載のシステム。

【請求項20】　前記制御手段が、第1のユーザの確認動作を成功裏に行ったと同時に、前記第1、第2および第3の指令を生じる前記メモリーに接続するマイクロプロセッサを含むことを特徴とする請求項18記載のカード。

【請求項21】　前記第1の指令がロード・キー指令であり、前記第2の指令が減分指令であり、前記第3の指令が読出し許容ブロック指令であることを特徴とする請求項20記載のカード。

【請求項22】　前記メモリーが更に、前記カードを正常な記憶動作を行うように条件付ける予め定めた指令セットを復号する指令制御手段を含み、前記指令制御手段が、前記第1、第2および第3の指令を含む別の指令セットを復号して前記メモリーに記憶された情報に対する機密保護を行う手段を含むことを特徴とする請求項18記載のカード。

【請求項23】　各々がアドレス指定可能な場所に構成されたメモリー・アレイを含む複数の不揮発性メモリー・チップと、記憶動作を行う指令信号を生じる制御論理回路を含むホスト・コンピュータに組込み可能な機密保護メモリー・カードを構成する方法において、
（a）組込まれた時前記ホスト・コンピュータと通信するように接続される前記カードにマイクロプロセッサを組込み、該マイクロプロセッサは、記憶域に対するユーザのアクセス可能性を定義する複数のキー値を含む情報と、前記記憶域に対するアクセス可能性を定義するメモリー構成情報とを記憶するためのアドレス指定可能な不揮発性メモリーを含み、
（b）機密保護論理回路を各不揮発性メモリー・チップに組込み、該機密保護論理回路が、予め定めたロック値を記憶する不揮発性ロック・メモリーと、該ロック・メモリーと接続されたアクセス制御論理手段と、前記構成情報に従ってアクセス可能性のビット情報を記憶する前記ブロック数と対応する複数の場所を有するアドレス指定可能な揮発性アクセス制御メモリーとを含み、
（c）前記マイクロプロセッサを各メモリー・チップに組込み、アドレスとデータと制御情報とを前記各メモリー・チップへ転送し、
（d）複数の指令に応答して前記機密保護論理回路を動作させるよう前記制御論理回路を修正し、
（e）前記ホスト・コンピュータと共に前記マイクロプロセッサによる初期の予め確立されたユーザ確認動作を実施し、
（f）ステップ（e）における前記確認動作が成功裏に行われた時にのみ、前記各チップに対して前記複数の指令の特定のものを転送する前記マイクロプロセッサにより前記機密保護論理回路を可能状態にして、前記ブロックの異なるものに記憶された前記情報を前記アクセス制御メモリーに記憶された前記アクセス可能性ビット情報に従って読出すことを許容するステップを含むことを特徴とする方法。

【請求項24】　前記マイクロプロセッサの不揮発性メモリーが複数のセクションを有し、ステップ（a）が更に、前記キー値に対する乱数を生成して該キー値を前記セクション数の最初のものにロードするステップを含むことを特徴とする請求項23記載の方法。

【請求項25】　前記マイクロプロセッサが更に、前記マイクロプロセッサの不揮発性メモリーに接続されたインターバル・カウンタを含み、ステップ（a）が更に、ユーザが選択した時間間隔を生成して該ユーザ選択時間間隔値と対応する値を前記インターバル・カウンタへロードするステップを含み、更に
（g）前記ユーザ選択時間間隔でステップ（e）の前記ユーザ確認動作を周期的に開始し、
（h）ステップ（b）の前記確認動作が成功裏に行われる限り、前記ブロックに記憶された前記情報が前記アク

セス可能性ビット情報に従って読出されることを許容し続けるステップを含むことを特徴とする請求項２４記載の方法。

【請求項２６】　各々がアドレス指定可能な場所のブロックに構成されたメモリー・アレイを含む多数の情報を記憶するための複数の不揮発性メモリー・チップと、記憶動作を行うための指令信号を生成する制御論理回路とを含む機密保護メモリー・カードを構成する方法において、

（ａ）記憶域に対するユーザのアクセス可能性を定義する多数のキー値を含む情報と、前記記憶域に対するアクセス可能性を定義するメモリー構成情報とを記憶するためのアドレス指定可能な不揮発性メモリーを含むマイクロプロセッサを前記カードに組込み、

（ｂ）予め定めたロック値を記憶する不揮発性ロック・メモリーと、該ロック・メモリーに接続されたアクセス制御論理手段と、前記構成情報に従ってユーザのアクセス可能性ビット情報を記憶する前記多数のブロックと数において対応する複数の場所を有するアドレス指定可能な揮発性アクセス制御メモリーとを含む機密保護論理回路を各不揮発性メモリー・チップに組込み、

（ｃ）アドレスとデータと制御情報とを前記各メモリー・チップへ転送するため前記マイクロプロセッサを各メモリー・チップに相互に接続し、

（ｄ）前記制御論理回路により通常与えられる１組の指令に対する拡張として前記機密保護論理回路を動作させる複数の指令を組込むように前記制御論理回路を修正することにより、前記機密保護論理回路が、前記多数のチップが前記メモリー・カードから取外される場合でも、前記チップに含まれる前記情報が不当な方法で読出されることを防護するステップを含むことを特徴とする方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、携帯用パーソナル・コンピュータの分野に関し、特に可搬性ディジタル情報環境におけるデータ機密保護のための保守システムに関する。

【０００２】

【従来の技術】個人情報の機密保護はいつまでも問題である。この個人情報は、ロック、コードおよびシークレット・ポケットにより保証されてきた。情報が新しい形態をとると、変化した状況に見合うように新しい方法が要求されてきた。

【０００３】歴史的には、情報の機密保護は，署名、印章および写真の使用により対処されてきた。自動銀行業務機械の如き電子装置は、コード化カードおよび個人の識別番号（ＰＩＮ）を機密保護ツールのレパートリに加えた。コンピュータ・システムは、パスワードを使用し続けている。

【０００４】特に、「スマート・カード」が機密保護ツールとして使用されている。この「スマート・カード」は、書込み可能な不揮発性メモリーと、１枚のチップとして作られプラスチック製「クレジット・カード」に組込まれた簡単な入出力インターフェースとを備えた小型マイクロコンピュータである。このカードは、特に設計された装置と接続することを可能にする外部バッドを有する。カードのマイクロコンピュータに保持されるプログラムは、この装置と対話して、その不揮発性メモリー・データをパスワードの交換を任意に含む所要のアルゴリズムに従って読出しあるいは修正することを可能にする。メモリー情報を保護しかつ状況に従って種々の許容を行う特殊な技法が実現されてきた。例えば、米国特許第４，３８２，２７９号「オンチップ修飾可能メモリーを備えた単一チップ・マイクロプロセッサ（Ｓｉｎｇｌｅ Ｃｈｉｐ Ｍｉｃｒｏｐｒｏｃｅｓｓｏｒ ｗｉｔｈ ｏｎ－Ｃｈｉｐ Ｍｏｄｉｆｉａｂｌｅ Ｍｅｍｏｒｙ）」は、処理および制御装置と同じチップに含まれる不揮発性メモリーの自動プログラミングを可能にするアーキテクチャを開示している。他のシステムにおけるように、マイクロプロセッサは単に同じチップ上のメモリーを保護するに過ぎない。

【０００５】「スマート・カード」は、識別のプロセスを容易にすると共に重要な情報を使えるようにするために用いられてきた。このような場合に、大半の過去の状況における如く、「キー」の物理的存在ならびにある特別な知識が、検証または確認プロセスの一部として用いられて来た。上記のこのような場合に、識別は、アクセスを要求する個人と機密保護ガードまたは自動出納機械の如き固定された機関との間の対話であった。

【０００６】自立する計算装置の可搬性の今日の状態は、物理的なキーと確認機関の両者を小型で可搬性のあるものにし、従って更に紛失または盗難が避けられなくなる。更に、計算装置は、識別プロセスと関連する特殊な知識またはパスワードを考えあるいは推論する試みを何度も行うことを可能にする。これは、確認機関または装置もまた泥棒または強盗の手中にある場合にも特に妥当する。更に悪いことには、技術は今や災難から免れないポケットまたはハンドバッグに大量の敏感な情報を携行することを許しかつ促すものである。

【０００７】今日では、ノートブックおよびサブノートブック・サイズのコンピュータが、著しい計算能力を許容しこのため更なるデータ格納容量の必要を生じる可搬性のある自立環境を提供する。このことは、最初はプログラムとデータの両方を保持する小型ハード・ディスク装置により遭遇した。パスワード保護は、これらのシステムにおいてしばしば用いられているが、第１に、確認機関自体が被害を受け易いため、敏感なデータを完全に保護するものではない。しかし、更に、データを保持するディスク・ドライブは、物理的に取外すことができ、

かつデータ分析を更に容易にする設定においてアクセスすることができる。この場合、ある形態の暗号化だけがデータの保護を可能にする。ディスク・アクセスの性質が、不当な行為もしくはコストの障壁なしにこれを可能にする。このような形式のシステムの一例は、米国特許第４，９８５，９２０号「集積回路カード（Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ　Ｃａｒｄ）」において記述されている。

【０００８】フラッシュ・メモリーおよび取外し可能「記憶カード」の最近の出現により、携帯型コンピュータの寸法および給電要件の大きな低減を可能にした。このフラッシュ・メモリーは、ランダム・アクセス・メモリー（ＲＡＭ）の柔軟性をディスクの性能に結付ける。今日では、これら技術の組合わせにより、紙を必要とすることなく２０，０００，０００バイトまでのデータをクレジット・カード・サイズの取外し可能パッケージに保有することを可能にする。このデータは、あたかも従来のディスク・ドライブに保持されるかのように、あるいはホストのメモリーの拡張であるかのようにホスト・システムから見えるにようにすることができる。これらの技術の進展は、ハンドバッグまたはブリーフケースよりもポケットで携行される如き程度までシステム・サイズの更なる減少を可能にした。

【０００９】このため、データおよびそのホスト・システムは、紛失または盗難を受け易くなると同時に、大きなコストおよび性能上の障壁となるため、暗号化によりメモリーのデータを保護することを更に困難にした。

【００１０】

【発明が解決しようとする課題】従って、本発明の主たる目的は、機密保護メモリー・サブシステムを備えた携帯型ディジタル・システムの提供にある。

【００１１】本発明の別の目的は、携帯型ディジタル・システムから取出されても保護することができるメモリー・カードの提供にある。

【００１２】本発明の更に他の目的は、かかるカードのチップが取出されても保護されるメモリー・カードの提供にある。

【００１３】

【課題を解決するための手段】上記の目的は、本発明の望ましい実施態様の機密保護カードにおいて達成される。この機密保護メモリー・カードは、単一の半導体チップ上のマイクロプロセッサと、１つ以上の不揮発性のアドレス指定可能なメモリー・チップとを含んでいる。このマイクロプロセッサ・チップおよび不揮発性メモリー・チップは、共にアドレス、データおよび制御情報をこのような不揮発性メモリー・チップへ送るための内部カード・バスに接続している。マイクロプロセッサは、内部バスにおけるアドレス、データおよび制御情報の転送を制御するための複数のキー値、構成情報およびプログラム命令情報を含む情報を記憶するためのアドレス指定可能な不揮発性メモリーを含む。チップ・メモリーは、各々が複数のアドレス指定可能な記憶場所を有する複数のブロック即ちバンクに構成される。

【００１４】本発明によれば、各メモリー・チップは、機密保護制御論理回路を含むように構成される。望ましい実施態様においては、これら回路は、マイクロプロセッサの制御下でロード可能な不揮発性ロック・メモリー、不揮発性ロック記憶可能化要素および揮発性アクセス制御メモリーを含む。更に、マイクロプロセッサは、第１に、ロック値を不揮発性ロック・メモリーにロードし、アクセスを禁止するロック記憶可能化要素をリセットする。その後、マイクロプロセッサは、構成情報により指定されるようにアクセス制御メモリーをロードする。このような情報は、ユーザがホスト・コンピュータによる予め定めた確認手順を成功裏に行ったことをマイクロプロセッサが判定した後にのみロードされる。各メモリーの機密保護論理回路は、メモリー・チップのアクセス制御メモリーにロードされた構成情報の関数として、フラッシュ・メモリーの選択されたアドレス指定可能なブロックに記憶された情報の読出しを可能化する。周期的に、ユーザはホスト・コンピュータによる確認手順をうまくゆくように行うことが要求され、またユーザはアクセス制御メモリーにより許容される如き情報の読出しを継続することが許される。望ましい実施態様においては、ホスト・コンピュータは、パーソナル・コンピュータ・メモリー・カード国際協会（ＰＣＭＣＩＡ）規格と合致するインターフェースの如き標準的インターフェースを介してメモリー・カードに接続される。

【００１５】本発明は、電子的な小型化が生成する「機密保護」環境におけるフラッシュ・メモリー技術により可能にされる大量のデータの保護を可能にするための要諦である「スマート・カード」と「メモリー・カード」技術を融合する。更に、本発明は、両技術における改善および強化を利用することができる。

【００１６】更に、本発明の機密保護論理回路は、フラッシュ・メモリーの基本的論理回路に対して行うことが要求される変更量を最小化するように、フラッシュ・メモリーに組込まれてこれと関連して動作する。更に、フラッシュ・メモリーは、機密保護モード、および機密保護論理回路がバイパスされてフラッシュ・メモリーがこの回路が組込まれなかったかのように動作することを可能にする非機密保護モードで動作することができる。通常、非機密保護モードには、フラッシュ・メモリーの不揮発性ロック・メモリー内容がクリヤされる時に入る。これは一般に、予め定めた状態（即ち、全て１の状態）に自然に消去するプログラムされないか完全に消去されたフラッシュ・メモリーを示す。

【００１７】少量のロジックをフラッシュ・メモリーおよび「アクセス制御プロセッサ（ＡＣＰ）」に加えることにより、フラッシュ・メモリーの内容はデータの暗号

化を必要とせずに機密保護される。従って、本発明は、大きなデータ・ブロックに対しては非常に時間を費やし得るデータの暗号化および解読のオーバーヘッドを排除する。

【００１８】動作において、ＡＣＰは、システムのユーザにある形態の確認の入力を周期的に促す。これは、パスワード、ＰＩＮ、特定のペン・コンピュータの筆記面上の特定点で行われる「ジェスチャ」、ユーザの音声による指令即ち「音声プリント」であり得る。方法はシステムによって異なる。プログラム可能ＡＣＰは、ユーザが確認の特定内容およびプロンプトの周期を変更することを許容する。ロックおよびアクセス制御メモリーにより要求される確認に対するコードおよびデータは、ＡＣＰと同じチップ上にあるＡＣＰ不揮発性メモリー内に記憶され、従って保護される。

【００１９】先に述べたように、良好な確認はＡＣＰをしてアクセスのためフラッシュ・メモリーの全てまたは選択されたブロックを可能状態にさせあるいは可能状態を継続させる。障害が、フラッシュ・メモリーに対するアクセスを不能にさせる。このため、この動作は、確認を良好に完了し損なうとフラッシュ・メモリーのデータを保護させることになる点において「デッドマン・スロットル」に類似している。更に、ユーザにより発された指令もまた、アクセスを不能にさせ得る。更に、給電オフ状態からの最初の給電と同時に、保護されたメモリー内容に対するアクセスは、最初の確認が成功裏に行われるまで阻止される。

【００２０】このため、メモリー・カードまたはそのホスト・プロセッサのいずれか一方が失われるか、盗まれるか、消勢されるか、あるいは接続されないままにおかれるならば、メモリーのデータは、即時あるいはその時の周期的確認が終了直後のアクセスから保護される。盗難の場合は、メモリー・データは、メモリー・カードが開路されて電子的にプローブされるか、あるいはメモリー・チップが取外されて別の装置に置かれても、アクセスから保護される。

【００２１】本発明の上記の目的および利点については、添付図面に関して以降の記述を読めば更によく理解されよう。

【００２２】

【実施例】図１は、パーソナル・コンピュータあるいはトランザクション・プロセッサとして使用可能な携帯可能な機密保護コンピュータ・システム１のブロック図である。システム１は、バス１０２によりホスト・プロセッサ５と接続する本発明により構成されたメモリー・カード３を含む。ホスト・プロセッサ５は、Ｈｅｗｌｅｔ－Ｐａｃｋａｒｄ社製のＨＰ９５ＬＸの如きパームトップ・パーソナル・コンピュータの形態をとり得る。ホスト・プロセッサ５は、全て共通にバス１０６と接続される液晶ディスプレイ（ＬＣＤ）５－２と、キーボード５－４と、マイクロプロセッサ５－６と、メモリー５－８と、直列インターフェース５－１０とを含む。メモリー５－８は、１Ｍバイトの読出し専用メモリー（ＲＯＭ）と、５１２Ｋバイトのランダム・アクセス・メモリー（ＲＡＭ）とを含む。

【００２３】メモリー・カード３とホスト・プロセッサ５との間の接続は、標準的バス・インターフェースを介して確立される。望ましい実施態様においては、バス１０２は、パーソナル・コンピュータ・メモリー・カード国際協会（ＰＣＭＣＩＡ）規格に合致している。バス１０２は、ホスト・プロセッサ５とメモリー・カード３間に標準的インターフェース・チップ１０４およびメモリー・カード・バス１０５を介してアドレス、制御およびデータ情報を送るための経路を提供する。バス１０２、１０５、１０６の各々は、データ・バス、制御バスおよびアドレス・バスを含み、全ての類似のバスを介する連続的な信号経路を提供する。例えば、バス１０５は、アドレス・バス１０５ａと、データ・バス１０５ｂと、制御バス１０５ｃとを含む。

【００２４】ＰＣＭＣＩＡバス規格は、メモリー・カード上のディスク・エミュレーションをサポートする規格からメモリー・データに対するランダム・アクセスを可能にする実質的に異なる規格へ展開した。本発明のメモリー・カードは、暗号化技術によらずにランダムな記憶場所に対する迅速なアクセスを行うことにより、この新しい規格をサポートする保護技術を提供する。メモリー・アレイからホストへデータを運ぶデータ経路を制御することにより、本発明のメモリー・カードは、時間を費やすバッファリング、暗号化あるいはこの経路における他の逐次処理を用いることなくデータを保護する。

【００２５】典型的には、ユーザは、キーボード５－４からシステム１を操作して、ディスプレイ５－２上に情報を表示してメモリー・カード３にファイル単位で記憶された情報を更新する表計算およびデータベース機能の如き典型的な動作を行う。ホスト・プロセッサ５は、アドレス情報をバス１０２に送出して情報を検索し、必要に応じて、この情報を更新してこれを必要なアドレスおよび制御情報とともにメモリー・カード３へ返送する。

【００２６】図１に示されるように、本発明のメモリー・カード３は、バス１０５と接続されたアクセス制御プロセッサ（ＡＣＰ）１０と、各々バス１０５と接続された複数（ｎ個の）のＣＭＯＳフラッシュ・メモリー・チップ１０３ａ乃至１０３ｎとを含む。ＡＣＰ１０は、典型的には「スマート・カード」において使用されるものと同じ形式の処理要素である。ＣＭＯＳフラッシュ・メモリー１０３ａ乃至１０３ｎは、Ｉｎｔｅｌ社製のフラッシュ・メモリー・チップの形態を呈するものでよい。例えば、これらは、８個の１２８Ｋバイト×８個のＣＭＯＳフラッシュ・メモリーを含むＩｎｔｅｌ　２８Ｆ００１ＢＸ　１Ｍと呼ばれるＩｎｔｅｌフラッシュ・メモ

リー・チップの形態のものでよい。このため、４Mバイトのフラッシュ・メモリー・カードは、３２個のＣＭＯＳフラッシュ・メモリーを含む、即ち、「ｎ」＝３２。

【００２７】（アクセス制御プロセッサ１０）図２は、望ましい実施態様のアクセス制御プロセッサ（ＡＣＰ）１０をブロック図の形態で示している。図示の如く、ＡＣＰ１０は、バス１０５と接続された保護不揮発性メモリー１０－２と、ランダム・アクセス・メモリー（ＲＡＭ）１０－４と、マイクロプロセッサ１０－６と、インターバル・カウンタ１０－８と、インターフェース・ブロック１０－１０とを含む。不揮発性メモリー１０－２は、確認情報およびプログラムを記憶する複数のアドレス指定された記憶場所を専用化する。更に、記憶域１０－２ａは、１つ以上の個人の識別番号（ＰＩＮ）、プロトコル・シーケンス、あるいはユーザがシステムに対してアクセスしたことを識別しかつ再確認のため使用される時間間隔値に加えてユーザがアクセスし得るフラッシュ・メモリー１０３ａ乃至１０３ｎにおけるブロックを識別するための他の識別情報を記憶する。

【００２８】記憶域１０－２ｂは、フラッシュ・メモリー１０３ａ乃至１０３ｎの各々の保護のため使用されるキー値またはフラッシュ・メモリー１０３ａ乃至１０３ｎの各々のここのブロックを保護するため使用されるコードを記憶する。

【００２９】記憶域１０－２ｃは、要求される確認操作を実行するため、また障害に対して予め設定された条件が満たされるならば、システムをクリヤするためのプログラム命令シーケンスを記憶する。あるプログラム命令は、ユーザの再確認が生じる時を確立するインターバル・カウンタ１０－８のセッティングをユーザが制御することを可能にする。この再確認間隔は、割込みと、ユーザにＰＩＮまたは他のパスワードを再び入れさせることによりユーザの同一性の検証を要求するホスト・プロセッサ５に対する割込みとの間の時間を定義する。インターバル・カウンタ１０－８は、バス１０２によりホスト・プロセッサ５からのクロック・パルスを受取り、作業環境に従ってユーザにより設定することができる。例えば、家庭において、ユーザはタイマーをオフにする（即ち、タイマーを最大値に設定する）か、あるいはタイマー間隔を１時間に設定することもできる。航空機において、保護を増すためにユーザはこのタイマーを１０分に設定することもできる。先に述べたように、ユーザは、「パワーオン」毎にこの間隔のセッティングを再検査するように促され、これにより周期的な再確認を強制して機密保護を実施する。

【００３０】（フラッシュ・メモリー１０３ａ乃至１０３ｎ）図３は、フラッシュ・メモリー１０３ａ乃至１０３ｎの詳細なブロック図である。メモリー１０３ｂ乃至１０３ｎはメモリー１０３ａと同一に構成されているため、メモリー１０３ａの詳細な論理回路のみが示される。

【００３１】フラッシュ・メモリー１０３ａは、基本的には２つのセクション、即ち、本発明の機密保護アクセス制御回路を含む１つのセクションと、フラッシュ・メモリーの基本的即ち標準的な論理回路を含む別のセクションとからなる。

【００３２】（機密保護アクセス制御セクション）図３から判るように、本発明の機密保護制御回路は、図示の如く配置された３２ビットのキー・レジスタと、３２ビット揮発性ロック・レジスタ３３と、１２ビット遅延カウンタ３２と、コンパレータ回路３９と、全て１検出信号回路３８と、不揮発性ロック・メモリー３５と、１ビット不揮発性ロック記憶可能化要素３６と、揮発性アクセス制御メモリー４３と、アクセス修正許容ＡＮＤゲート３４と、出力ＯＲゲート４５とを含む。このセクションは、基本的論理セクションに含まれる指令レジスタ５０からの種々の16進数値（例えば、３１Ｈ乃至３８Ｈ）により示される指令制御信号を受取ることに注目されたい。これらの信号は、ＡＣＰ１０からデータ・バス１０５ｂを介して指令レジスタ５０により受取られる指令セットの異なるデータ値を表示する。これらの指令は、通常フラッシュ・メモリーにより使用される指令セットに対する重要な拡張である。標準的フラッシュ・メモリー指令は、２８Ｆ００１ＢＸフラッシュ・メモリーにより用いられる指令の形態をとる。これら指令については、参考のため本文に援用されるＩｎｔｅｌ社の「メモリー製品（Ｍｅｍｏｒｙ　Ｐｒｏｄｕｃｔｓ）」に記載されている。本発明により使用される指令は、表１に記載されている。

【００３３】表１に示される最初の指令は、乱数生成ロック値をメモリー１０３ａ乃至１０３ｎの各々における不揮発性ロック・メモリー（ＬＭ）３５へ最初にロードするため使用されるロード・ロック・メモリー指令である。メモリー１０３ａ乃至１０３ｎの各々は、ユーザの機密保護の必要に従って異なるロック値または同じロック値を有する。このロック値は、１ビット不揮発性ロック記憶要素３６の制御下でキー（Ｋ）レジスタ３１を介してＬＭ３５へロードされる。表１のリセット・ロック記憶可能化指令は、記憶要素３６のリセットに用いられる。これは、リセット・ロック記憶可能化指令により一旦リセットされた記憶要素３６はセットできないため、ＬＭ３５に記憶されたロック値が変更されることを阻止する。ＬＭ３５の不揮発性の内容は、パワーアップと同時にＬレジスタ３３へ送られる。ロック・メモリー３５の場所即ちサイトが設計に依存することが判るであろう。例えば、メモリー３５は、メモリー・アレイ５４に対する拡張として構成することができる。

【００３４】表１のロード・キー・レジスタ指令は、キー（Ｋ）レジスタ３１をロードしかつ遅延カウンタ３２をセットするために使用される。この減分遅延カウンタ

15　　16

の指令は、遅延カウンタ３２の内容を１だけ減分するためＡＣＰ１０により使用される。読出し許容メモリー・バンクおよび読出し不能化メモリー・バンク指令は、アクセス制御メモリー４３のロード中メモリー・アレイ５＊４の異なるメモリー・ブロックに対するアクセスを可能化あるいは不能化するためＡＣＰ１０により使用される。

【００３５】

表　１

指　令	第１バス・サイクル動作	アドレス日付	第２バス・サイクル動作アドレス	日　付
ロック・メモリーロード	書込み	３１Ｈ	書込み	Ｎ／Ａ
ロック・記憶可能化リセット	書込み	３３Ｈ	Ｎ／Ａ	Ｎ／Ａ
キー・レジスタロード	書込み	３２Ｈ	書込み	キー日付
遅延カウンタ減分	書込み	３５Ｈ	Ｎ／Ａ	Ｎ／Ａ
メモリー・バンク読出し許容	書込み	ＭＢＡ　３４Ｈ	書込み	ＭＢＡ
メモリー・バンク読出し不能化	書込み	ＭＢＡ　３８Ｈ	書込み	ＭＢＡ

ロック・メモリーをロード（３１Ｈ）

この指令は、ロック記憶可能化要素３６の出力信号が「真」である場合のみ、キー・レジスタ３１の内容を不揮発性ロック・メモリー３５へコピーする。

【００３６】ロック記憶可能化をリセット（３３Ｈ）

この指令は、ロック記憶可能化論理要素３６をリセットして、これによりロック・メモリー３５のロードまたは変更を禁止する。

【００３７】キー・レジスタをロード（３２Ｈ）

この指令は、キー・レジスタ３１の前の内容を１バイト（ＬＳＢからＭＳＢへ）だけシフトし、ＡＣＰ１０からの「キー値」をキー・レジスタのＬＳＢにロードする。更に、この指令は遅延カウンタ３２をその最大値、例えば全て「１」にセットする。

【００３８】遅延カウンタを減分（３５Ｈ）

この指令は、遅延カウンタ３２を１だけ減分する。遅延カウンタは、メモリー・アレイ５４の以降の読出しを許容するには「０」と等しくなければならない。

【００３９】メモリー・バンクを読出し許容（３４Ｈ）

この指令は、アクセス修正許容信号３７が「真」であるならば、アクセス制御メモリー４３におけるメモリー・バンク・アドレス（ＭＢＡ）と対応するビットをセットする。これは、選択されたバンクへの読出しアクセスを許容する。

【００４０】

メモリー・バンクを読出し不能化（３８Ｈ）

この指令は、アクセス制御メモリー４３におけるメモリー・バンク・アドレスと対応するビットをリセットする。

【００４１】表１を更に詳細に考察すれば、表１が加えられた指令の各々に対するバス・サイクル動作をも示すことが判る。２バス・サイクルを要求する各指令に対して、最初のバス・サイクル毎に、指令レジスタ５０がＡＣＰ１０により生じ、バス１０５のデータ・バス１０５ａおよび入力バッファ５１を介して送られた８ビット指令を受取る。指令レジスタ５０は、２番目のバス・サイクルの間選択された論理要素がデータ・バス１０５ｂから指令を実行するため必要な情報を受取るよう条件付けする。明らかなように、リセット・ロック記憶可能化および減分遅延カウンタ指令が実行のために１サイクルのみを必要とするため、この２番目のバス・サイクルは、使用不能（Ｎ／Ａ）と表示される。

【００４２】正常動作中、Ｋレジスタ３１は、ロード・キー・レジスタ指令により記憶場所１０－２ｂから受取ったキー値でロードされ、遅延カウンタ３２はその最大値にセットされる。遅延カウンタ３２は、ＡＣＰ１０から受取る連続的な減分遅延カウンタ指令に応答して全て「ゼロ」に減分され、ＡＮＤ３４に入力として与えられるゼロ・カウント出力信号４１を生じる。

【００４３】各遅延カウンタ３２は、泥棒がチップを外してこれらを「違法カード」に取付けて各メモリー・チップのキーを推理するためプロセッサ即ち装置を反復的

に試行するようにプログラムする場合に、フラッシュ・メモリー１０３ａ乃至１０３ｎをアクセスするため行うことができる試行即ち試みの回数を制限する。換言すれば、カウンタ３２は、フラッシュ・メモリーに対する不法なアクセスを獲得するために非常に多くの回数の試行即ち試みを行わねばならないことを保証する。キーおよび遅延カウンタのサイズは、このような試みが異常な時間を要することを必要とするように選択される。

【００４４】更に、キー・レジスタ３１は、略々四十億（2^{32}）の異なる組合わせを記憶する。望ましい実施態様においては、遅延カウンタ３２は１２ビット・カウンタである。遅延カウンタ３２がマイクロ秒毎に１回減分されるものとすれば、キー値の推論の試み毎に2^{12}即ち４ミリ秒を要することになる。正しいキー値を知るＡＣＰ１０は、最初のセットアップにおいて４ミリ秒の遅れを生じるに過ぎない。キー値を推理するランダムな試みは、５０％の成功率を得るためには2^{31}回の試みを必要とする。これは、キー値を推理するために$2^{31}\times2^{12}$ミリ秒、即ち１０２日を要する。この時間は、大半の泥棒を諦めさせるに充分である。無論、キーおよび遅延カウンタ３２のサイズを修正することにより、より長いか短い時間を与えることも可能である。

【００４５】本発明のメモリー・カードが盗まれて「不法なホスト」に取付けられる場合には、ＡＣＰ１０は、既知の手法でＰＩＮを推理する泥棒の試み回数を制限する。このような手法は、不当な推理の閾値を越えるならば、アクセスをロックするかあるいはデータを破壊することを含み得る。

【００４６】フラッシュ・メモリー１０３ａに対する最初の確認動作中、キー値は、４回連続するロード・キー・レジスタ指令に応答してキー値が３２ビットのＫレジスタ３１へロードされる（即ち、データ・バス１０５ｂが１バイト幅のバスである）。遅延カウンタ３２は、連続する最初のバス・サイクルにおいて減分遅延カウンタ指令を送るＡＣＰ１０により（全て「１」の）その最大カウントに強制されて減分される。遅延カウンタ３２は「０」に減分されると、ＡＮＤゲート３４の１つの入力に与えられるゼロ・カウント信号４１を生成する。

【００４７】Ｋレジスタ３１に記憶されたキー値が対応するＬレジスタ３３に記憶されたロック値と等しくユーザが正しい識別をホスト・プロセッサ５へ与えたことを示すならば、比較ロジック３９が等価比較信号４２をＡＮＤゲート３４の別の入力へ与える。これは、ＡＮＤゲート３４をしてその出力にアクセス修正許容信号３７を生じさせ、これがＡＣＰ１０の制御下でアクセス制御メモリー４３に対する書込みを可能化する。これは更に、メモリー・アレイ５４の読出しを後で許容する。

【００４８】アクセス制御メモリー４３は、メモリー・アレイ５４の各ブロック／バンクに対して１ビットの揮発性記憶域を保持する。これらのビットは、フラッシュ・メモリーのパワーアップ・シーケンスの一部として「ゼロ」にクリヤされる。データがメモリー１０３ａから読出されるためには、アドレス指定されたメモリー・ブロックと対応するビットが論理値「１」でなければならない。これらビットは、アクセス修正許容信号３７が「真」である場合にのみＡＣＰ１０によりセットされて読出し許容修正許容信号３７を生じる。

【００４９】表１に示されるように、読出し許容メモリー・バンク指令の２番目のバス・サイクルの間、メモリー・アレイ５４の選択されたメモリー・バンクの３つの上位アドレス・ビットがアドレス・バス１０５ｃに送出されると共に、16進数の指令識別子の反復がデータ・バス１０５ａを介して指令レジスタ５０へ送られる。その結果、「１」がアクセス制御メモリー４３におけるアドレス指定されたビット場所へ書込まれることになる。望ましい実施態様においては、メモリー・アレイ５４がそれぞれ１６Ｋバイトの８つのバンクに構成されるため、読出し許容メモリー・バンク指令シーケンスが８回繰返される。ＡＣＰ１０は、類似の方法で読出し不能化メモリー・バンク指令のシーケンスを発することにより選択されたバンクに対するアクセスを制限することもできる。

【００５０】本発明のアクセス制御メモリー４３の出力は、メモリー・アレイ５４のどれかのバンクの記憶域の内容が読出されつつある各フラッシュ・メモリー読出しサイクルの間、出力バッファ５２に対して可能化入力として与えられる。即ち、１読出しサイクルが生じるが、適当なバンクのアクセス制御メモリーのゲート信号のない時は読出されたデータが出力バッファ５２を通過することが禁止される。特に、望ましい実施態様の場合は、アクセス制御メモリー４３は、８つの個々にアドレス指定可能なビット記憶要素と、各記憶要素の入力に接続された入力アドレス３乃至８ビット・デコーダと、各記憶要素の出力の接続された１乃至８出力マルチプレクサ回路とを含む。各アドレスの３つの上位アドレス・ビットは、復号されてその内容が変更されるべきブロックに対する記憶要素を選択するため使用される。同様に、同じ３ビットが、読出されるフラッシュ・メモリーの記憶域を含むブロックに対する記憶要素の出力を選択するため使用される。

【００５１】ロック・メモリー３５が完全に消去される、即ち全て「１」のＬレジスタ３３の内容により示される如き全て「１」であるならば、出力バッファ５２は常に可能状態になる。即ち、ロック・レジスタ３３が「全て１」を含む時、これは「全て１」検出要素３８からＯＲゲート４５に対する信号を生成して出力バッファ５２を可能状態にする。これは、フラッシュ・メモリー１０３ａを有効に非機密保護モードに置く。これは、本発明の全ての機密保護論理回路をバイパスさせる。従って、同じフラッシュ・メモリー・チップを機密保護およ

19

び非機密保護の両用途に使用することができ、これにより生産経済をもたらす結果となる。

【００５２】（フラッシュ・メモリーの基本論理回路）図３および図４に示されるように、この回路は、メモリー・アレイ５４と、指令レジスタ５０と、入出力論理回路６０と、アドレス・ラッチ５６と、書込み状態マシン６１と、消去電圧システム６２と、出力マルチプレクサ５３と、データ・レジスタ５１と、出力バッファ５２と、状態レジスタ５８とを図のように含む。フラッシュ・メモリー１０３ａの基本論理回路は先に述べたように、Ｉｎｔｅｌ社製の２８Ｆ００１ＢＸと呼ばれるフラッシュ・メモリーに含まれる回路形式の形態をとる。こ＊

20

＊のような回路は周知であるため、必要な程度に述べるに止める。この回路に関するこれ以上の情報については、文献「メモリー製品（Ｍｅｍｏｒｙ　Ｐｒｏｄｕｃｔｓ）」（注文番号２１０８３０、Ｉｎｔｅｌ社１９９２年発行）の３－１０９乃至３－１３４ページを参照されたい。図３および図４に示されるように、フラッシュ・メモリーの基本回路は、多数の入力信号（Ａ０～Ａ１６）、アドレス、データ信号（Ｄ００～Ｄ０７）および制御信号（ＣＥ、ＷＥ、ＯＥ、ＰＷＤおよびＶＰＰ）を受取る。これら信号については、表２において以降に記述する。

【００５３】

表　２

記　号	名前および機能
Ａ０～Ａ１６	メモリー・アドレスに対する「アドレス入力」。アドレスは書込みサイクルの間内部的にラッチされる。

【００５４】Ｄ００～ＤＪ０７　「データ入出力」：メモリー書込みサイクル間の入力データおよび指令はメモリーおよび状態読出しサイクルの間データを出力する。データ・ピンはハイのアクティブ状態にあり、チップが選択から外されるか出力が消勢される時、３状態のオフへフロートする。データは書込みサイクルの間内部的にラッチされる。

【００５５】ＣＥ　チップ可能化：装置の制御ロジック、入力バッファ、デコーダおよび検出増幅器を付勢する。ＣＥはローのアクティブ状態であり、ＣＥハイが記憶装置の選択を外して、電力消費を待機レベルに低減する。

【００５６】ＰＷＤ　パワーダウン：装置を深いパワーダウン・モードに置く。ＰＷＤがローのアクティブ状態にあり、ＰＷＤハイが正常な動作をゲートする。ＰＷＤ＝ＶＨＨは、メモリー・ブロックのプログラミングを可能にする。ＰＷＤはんた、ローのアクティブ状態にある時消去または書込み動作をロックして、電力の供給中にデータ保護を行う。

【００５７】ＯＥ　出力可能化：　読出しサイクルの間装置の出力をデータ・バッファを通るように装置の出力をゲートする。ＯＥはローにアクティブ状態にある。

【００５８】ＷＥ　書込み可能化：指令レジスタ置くアレイ・ブロックへの書込みを制御する。ＷＥはローのアクティブ状態にある。アドレスおよびデータは、ＷＥパルスの立上がりエッジと同時にラッチされる。

【００５９】Ｖｐｐ　アレイの消去ブロックあるいは各ブロックのプログラミング・バイトに対する消去／プログラム給電。注：Ｖｐｐ＜Ｖｐｐ１　Ｍａｘの時、メモリー内容は変更できない。

【００６０】表２に示されるように、チップ可能化（ＣＥ）、書込み可能化プロセッサ（ＷＥ）および出力可能化（ＯＥ）の諸信号は、ホスト・プロセッサ５からバス１０２置く制御バス１０５ｂを介して指令レジスタ５０および入出力論理回路６０へ与えられ、制御指定論理ブロックへ分散される。パワーダウン（ＰＷＤ）信号もまた、フラッシュ・メモリーが表２で指定された諸動作を行うことを可能にするため指令レジスタ５０へ与えられる。この信号は、必要に応じてフラッシュ・メモリーの機密保護制御セクションの揮発性記憶要素をクリヤするため使用することができ、これにより正常な動作が再び再開されると、ユーザの再確認を強化する。

【００６１】一般に、フラッシュ・メモリーの基本論理要素は下記のように動作する。情報は、アドレス・バス１０５ｃからのアドレス・ロジック５６により受取られるアドレスにより指定されるメモリー・ブロックの１つのアドレス指定された場所におけるデータ・バス１０５ａ、入力バッファ５１およびデータ・レジスタ５５を介してメモリー・アレイ５４に記憶される。情報は、メモリー・アレイ５４のバンクの指定されたアドレス場所から読出され、出力マルチプレクサ５３、出力バッファ５２、データ・バス１０５ａおよびバス１０２を介してホスト・プロセッサ５へ送られる。状態レジスタ５８は、書込み状態マシンの状態、エラー中断状態、消去状態、プログラム状態およびＶｐｐ状態を記憶するために使用される。

【００６２】書込み状態マシン６１は、ブロックの消去を制御しかつプログラムのアルゴリズムを制御する。プログラム／消去電圧システム６２は、Ｖｐｐのレベルの関数として、メモリー・アレイ５４のブロックまたは各ブロックのプログラミング・バイトの消去のため使用される（即ち、Ｖｐｐがハイのレベルにある時、プログラミングが生じ得る；Ｖｐｐがローのレベルならば、メモリー・アレイ５４は読出し専用メモリーとして機能する）。

【００６３】（動作の記述）本発明の機密保護メモリー・カードの動作については、特に図５、図６および図７のフロー図に関して以下に述べる。このような動作を詳

細に述べる前に、メモリー・カードの製造、特別調製および動作に含まれる諸ステップについて最初に述べることにする。

【００６４】最初のステップとして、カードの製造時に、ＡＣＰ１０はメモリー・カード上の各メモリー・チップに対するロック値をセットする。ＡＣＰ１０は、キー値を図３および図４のロック・メモリーへロードすることによりこれを行う。これらの値は、ＡＣＰの保護不揮発性メモリー１０－２（即ち、図２におけるキー１～ｎ）に記憶される。次にロック記憶可能化論理要素３６がゼロにセットされて、ロック・メモリーの内容のこれ以上の変更または読出しを禁止する。これら要素が不揮発性であるため、フラッシュ・メモリー・チップ全体がクリヤされなければ、変更することができない。

【００６５】第２のステップとして、用途の特別調製時に、書込みが保護の機能により影響を受けないため、メモリー・カードはそのデータまたはソフトウエア・アプリケーションでロードすることができる。この時、ＡＣＰ１０はメモリーのバンク構造および各メモリー・バンクに与えられるべき保護の程度に関する情報でロードされる。

【００６６】第３のステップとして、ユーザの特別調製時に、ユーザは確認データおよび要求される特定データの周期およびモードに対するパラメータ（例えば、個人識別番号（ＰＩＮ））を確立する。

【００６７】第４のステップとして、パワーオン時に、「キー・レジスタ」、「アクセス修正許容」信号および「アクセス制御メモリー」が初期設定されて、アクセス制御メモリー４３に対するデータ・アクセスまたは書込みを禁止する。最初の確認対話が開始される。

【００６８】最初の確認対話時に、ＡＣＰ１０は、そのホスト・プロセッサ５のサービスを用いてユーザを促して確認情報を受取る。確認が不成功であれば、動作は行われず、成功すれば、各々メモリー・チップのキー・レジスタがＡＣＰのメモリーに記憶された値でロードされる。この動作中、遅延カウンタ３２が、成果のないプロセス乱打むな試みを行う以降のローディングの期間中チップの動作を禁止するため用いられるキー・レジスタのローディングは、「アクセス修正許容」信号を各チップにおいて真にさせる。その時、ＡＣＰ１０は、記憶された情報の構成に従ってアクセス制御メモリーをロードすることによりアクセスを確立する。

【００６９】６番目のステップとして、以降の確認対話時に、ユーザの構成に従って、ＡＣＰ１０が別のユーザの確認（再確認）を促す。失敗の場合、ＡＣＰ１０は全てのメモリー・チップをそれらのパワーオン状態に強制し、これによりアクセス制御メモリー４３をクリヤしかつキー・レジスタ３１の内容をクリヤすることによりメモリーのデータに対するアクセスを禁止する。次に、図１のシステムの動作について図５、図６および図７に関して記述する。

【００７０】（遅延の最初の動作）図５および図６は、種々の動作モードをブロック図形態で示している。ブロック４０２および４０１は、２つの始動条件を示す。ブロック４０２において、ユーザはメモリー・カード３を前にパワーアップされたホスト・プロセッサ５に挿入する。ブロック４０１において、ユーザはホスト・プロセッサ５を既に組込んだメモリー・カード３でパワーアップする。

【００７１】上記の始動動作のいずれかにおいて、ブロック４０２の間、ＡＣＰ１０およびそのインターフェースが従来周知の方法で初期設定され、ブロック４０３が「ｎ」個のＫレジスタ３１と「ｎ」個のアクセス制御メモリー４３をフラッシュ・メモリー１０３ａ乃至１０３ｎの全てを内部初期設定シーケンスの一部としてクリヤする。これは、各メモリーにおける出力バッファ５２が不能化されるため、メモリー１０３ａ乃至１０３ｎからデータが読出されることを阻止する。ロック値が、パワーオンの結果として各ＬＭ３５から「ｎ個の」Ｌレジスタ３３にロードされる。

【００７２】次にブロック４０４において、ＡＣＰ１０は、ユーザからＰＩＮまたは他の識別情報を要求することにより応答するホスト・プロセッサ５へ割込み信号を送る。ブロック４０５において、ＡＣＰ１０は、メモリー記憶域１０－２ａに記憶されたプログラムにより、前記ＰＩＮまたは他の識別情報がメモリー記憶域１０－２ａに記憶された情報と一致することを調べる。もし一致しなければ、判断ブロック４０６がエラーをカウントして、ＡＣＰ１０がブロック４０４へ分岐しテストを反復する。テストが予め設定された回数失敗するならば、判断ブロック４０６はブロック４０７へ分岐してＡＣＰ１０をしてメモリー１０３ａ乃至１０３ｎの内容をロックアップあるいは破壊させる。

【００７３】（成功した最初のユーザ確認）判断ブロック４０６において成功した確認を示す一致があるならば、ブロック４０８において、ＡＣＰ１０がロード・キー・レジスタ指令を介して、各Ｋレジスタ３１を記憶場所１０－２ｂから適当なキー値でロードする。また、ブロック４０９は遅延カウンタ３２の内容を反復的に減分して、減分遅れカウンタ指令を２進数ゼロのカウントになるよう連続的に発行し、これが図３および図４におけるゼロ・カウント信号４１の生成を生じる。

【００７４】ブロック４１０において、アクセス制御メモリー４３の各記憶域が読出し許容メモリー・バンク指令により情報がロードされて、対応するフラッシュ・メモリー１０３ａ乃至１０３ｎの選択されたバンクへのアクセスを許容する。

【００７５】（間欠的な再確認）ブロック４１１において、ＡＣＰ１０は、ユーザの再確認を要求する前に、インターバル・カウンタ１０－８により信号される記憶域

１０－２に記憶された情報により確立される予め設定された時間間隔の終りを待機する。次いで、ブロック４１２において、ＡＣＰ１０は、ホスト・プロセッサ５に割込みをかけてユーザがＰＩＮまたは他の要求される識別を再入力することを要求する。

【００７６】判断ブロック４１３は、ホスト・プロセッサ５から受取ったＰＩＮまたは他の情報を記憶域１０－２ａに記憶された情報に対して検査し、インターバル・カウンタ１０－８出力が記録される。ユーザは、確認情報をホスト・プロセッサ５に入力する典型的に３０秒の予め設定された時間間隔を有する。クロックが作動し続ける間、判断ブロック４１３のテストが失敗すると、ブロック４１４がこのテストをエラーとして記録する。この時、これは、最大数のエラーが受取られたかどうかを調べ、ブロック４１２および４１３を反復するため分岐する。エラー数が最大数と等しければ、ブロック４１５において、ＡＣＰ１０は連続的なロード・キー・レジスタ指令によりフラッシュ・メモリーのＫレジスタ３１をクリヤし、連続的な読出し不能化メモリー指令によりアクセス制御メモリー４３をクリヤする。次にブロック４１５は、ブロック４０４へ分岐して新しい「最初の確認」動作が生じることを許容する。

【００７７】判断ブロック４１３におけるテストが成功するならば、Ｋレジスタ３１は変化しないままであり（即ち、ＡＣＰにより前にロードされたキー値を保持する）、ユーザがシステム１を動作させ続けることを可能にする。判断ブロック４１３がＰＩＮまたは他の情報を受取ることなく３０秒が経過した場合、ＡＣＰ１０は前のようにＫレジスタ３１とアクセス制御メモリー４３とをクリヤする。

【００７８】図７は、図５および図６のブロック４０４および４１２に応答して、ホスト・プロセッサ５がどのようにＡＣＰ１０からの割込み要求に応答するかを示すフロー図である。図示の如く、判断ブロック５０１は、ユーザがＰＩＮまたは他の情報を再入力することを要求するＡＣＰ１０からの割込みを待機する。判断ブロック５０１は、ブロック４０４または４１２から割込みを受取る時ブロック５０２へ分岐する。ブロック５０２は、ホストのディスプレイ５－２におけるＰＩＮまたは他の情報に対する要求を表示する。ブロック５０３は、キーボードからの情報を受入れ、ブロック５０４はＡＣＰ１０に割込みをかける。ブロック５はＡＣＰ１０に対してＰＩＮを送出する。

【００７９】当業者には、本発明の教示から逸脱することなく本発明の望ましい実施態様に多くの変更が可能であることが判るであろう。例えば、本発明は、異なる形式の不揮発性メモリーおよび異なるインターフェースなどと共に用いることができる。

【００８０】法規に従って本発明の最善の形態を記し示したが、頭書の特許請求の範囲に記載したように本発明の趣旨から逸脱することなく変更が可能であり、ある場合には、本発明のある特徴を他の特徴に関わることなく有利に用いることができる。

【図面の簡単な説明】

【図１】本発明により構成されたメモリー・カードを組込んだシステムを示す全体ブロック図である。

【図２】不揮発性メモリーのレイアウトを含む図１のアクセス制御プロセッサ（ＡＣＰ）を更に詳細に示すブロック図である。

【図３】本発明により修正された図１の標準的なフラッシュ・メモリーを示す更に詳細なブロック図である。

【図４】本発明により修正された図１の標準的なフラッシュ・メモリーを示す更に詳細なブロック図である。

【図５】種々の確認手順を実施する際の本発明のメモリー・カードの動作を説明するため用いられるフロー図である。

【図６】種々の確認手順を実施する際の本発明のメモリー・カードの動作を説明するため用いられるフロー図である。

【図７】種々の確認手順を実施する際の本発明のメモリー・カードの動作を説明するため用いられるフロー図である。

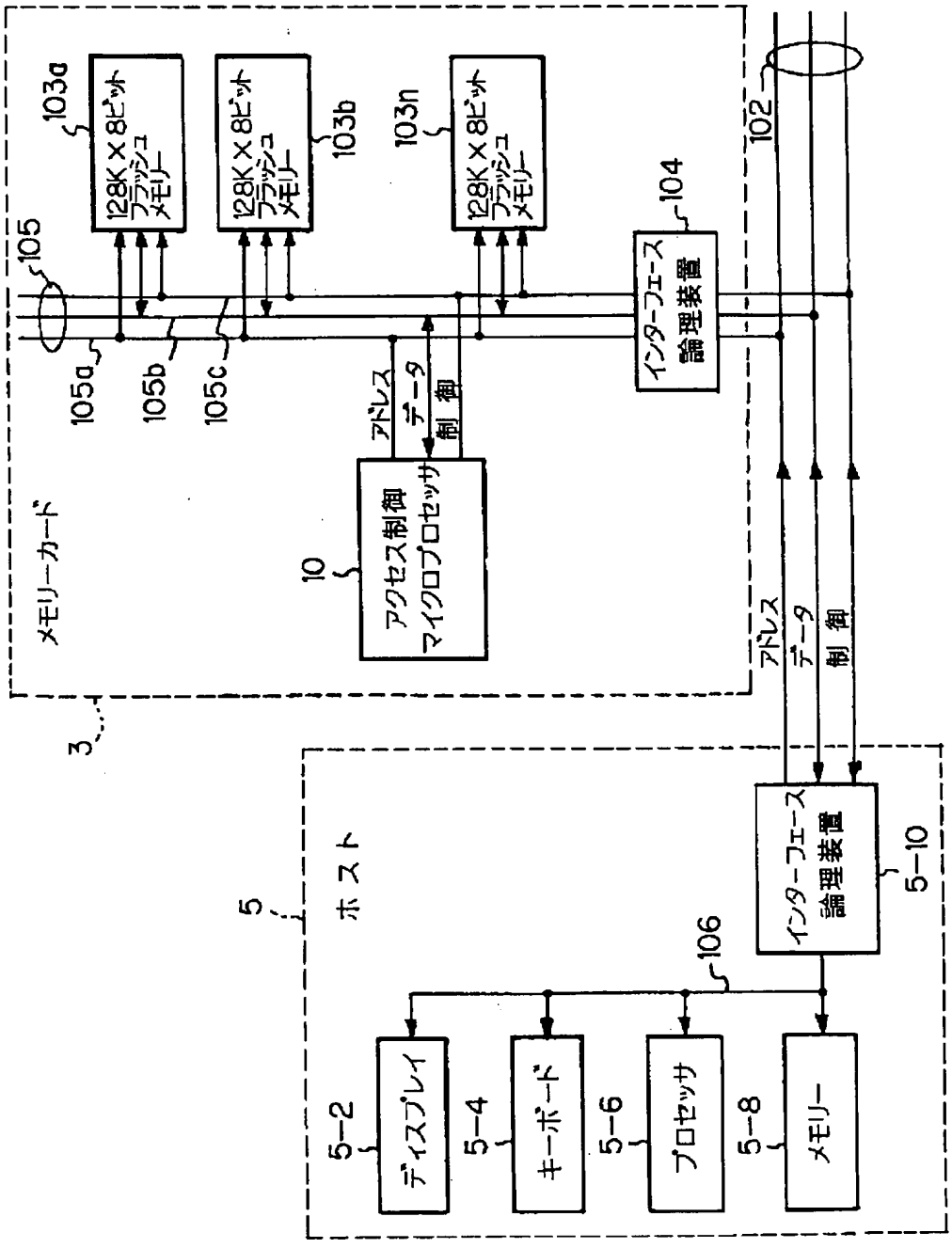
【符号の説明】

１　携帯可能な機密保護コンピュータ・システム
３　メモリー・カード
５　ホスト・プロセッサ
５－２　液晶ディスプレイ（ＬＣＤ）
５－４　キーボード
５－６　マイクロプロセッサ
５－８　メモリー
５－１０　直列インターフェース
１０　アクセス制御プロセッサ（ＡＣＰ）
１０－２　保護不揮発性メモリー
１０－４　ランダム・アクセス・メモリー（ＲＡＭ）
１０－６　マイクロプロセッサ
１０－８　インターバル・カウンタ
１０－１０　インターフェース・ブロック
１０－１２　インターフェース論理装置
３１　キー（Ｋ）・レジスタ
３２　１２ビット遅延カウンタ
３３　３２ビット揮発性ロック・レジスタ
３４　アクセス修正許容ＡＮＤゲート
３５　不揮発性ロック（Ｌ）・メモリー
３６　１ビット不揮発性ロック記憶可能化要素
３７　アクセス修正許容信号
３８　全て１検出信号回路
３９　コンパレータ論理回路
４１　ゼロ・カウント信号
４２　等価比較信号
４３　揮発性アクセス制御メモリー

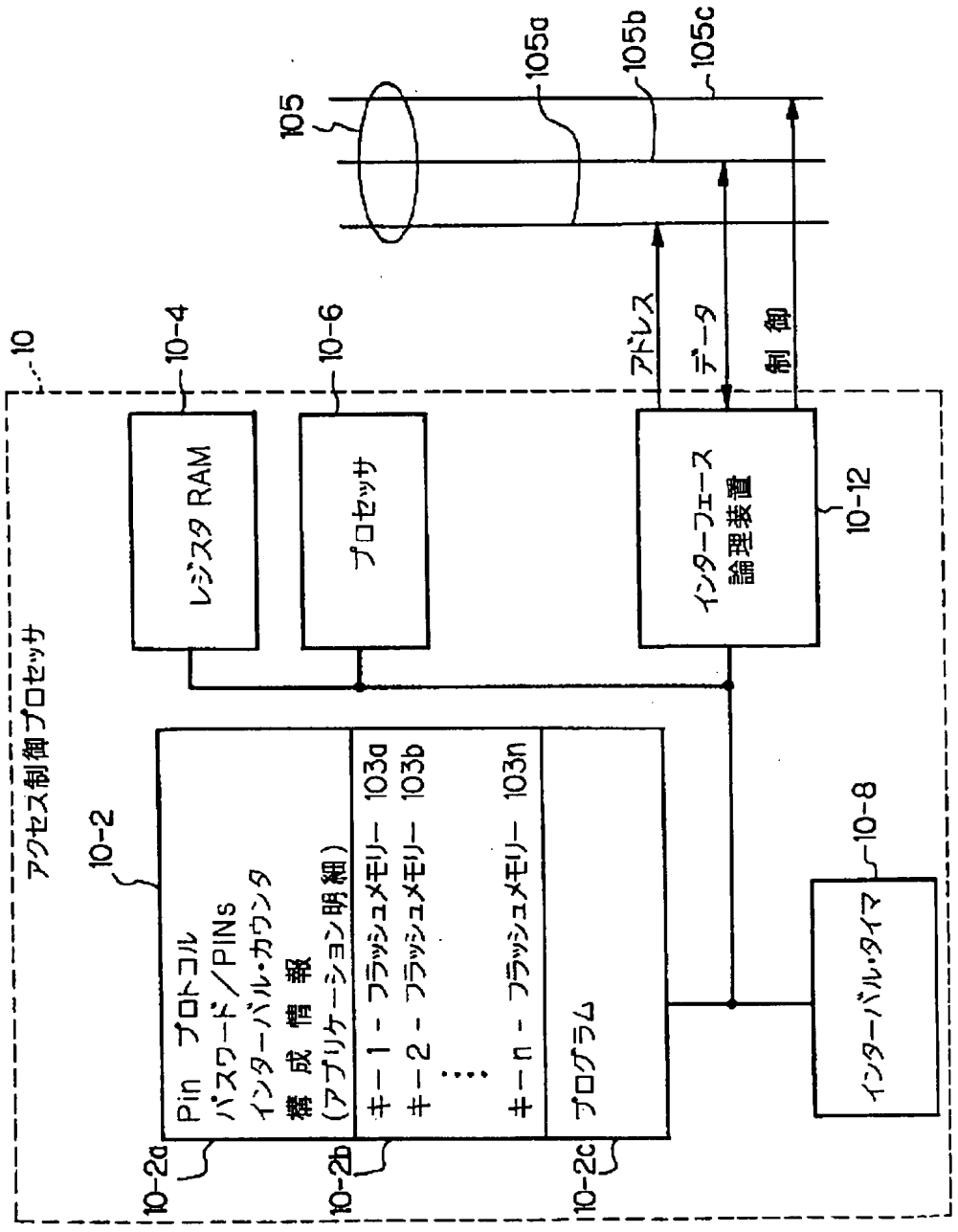
25　　26

４５　出力ＯＲゲート
５０　指令レジスタ
５１　データ・レジスタ
５２　出力バッファ
５３　出力マルチプレクサ
５４　メモリー・アレイ
５６　アドレス・ラッチ
５８　状態レジスタ
＊６０　入出力論理回路
６１　書込み状態マシン
６２　プログラム／消去電圧システム
１０２　バス
１０３ａ～ｎ　１２８Ｋ×８ビットＣＭＯＳフラッシュ・メモリー・チップ
１０４　標準的インターフェース論理装置
＊　１０５　メモリー・カード・バス

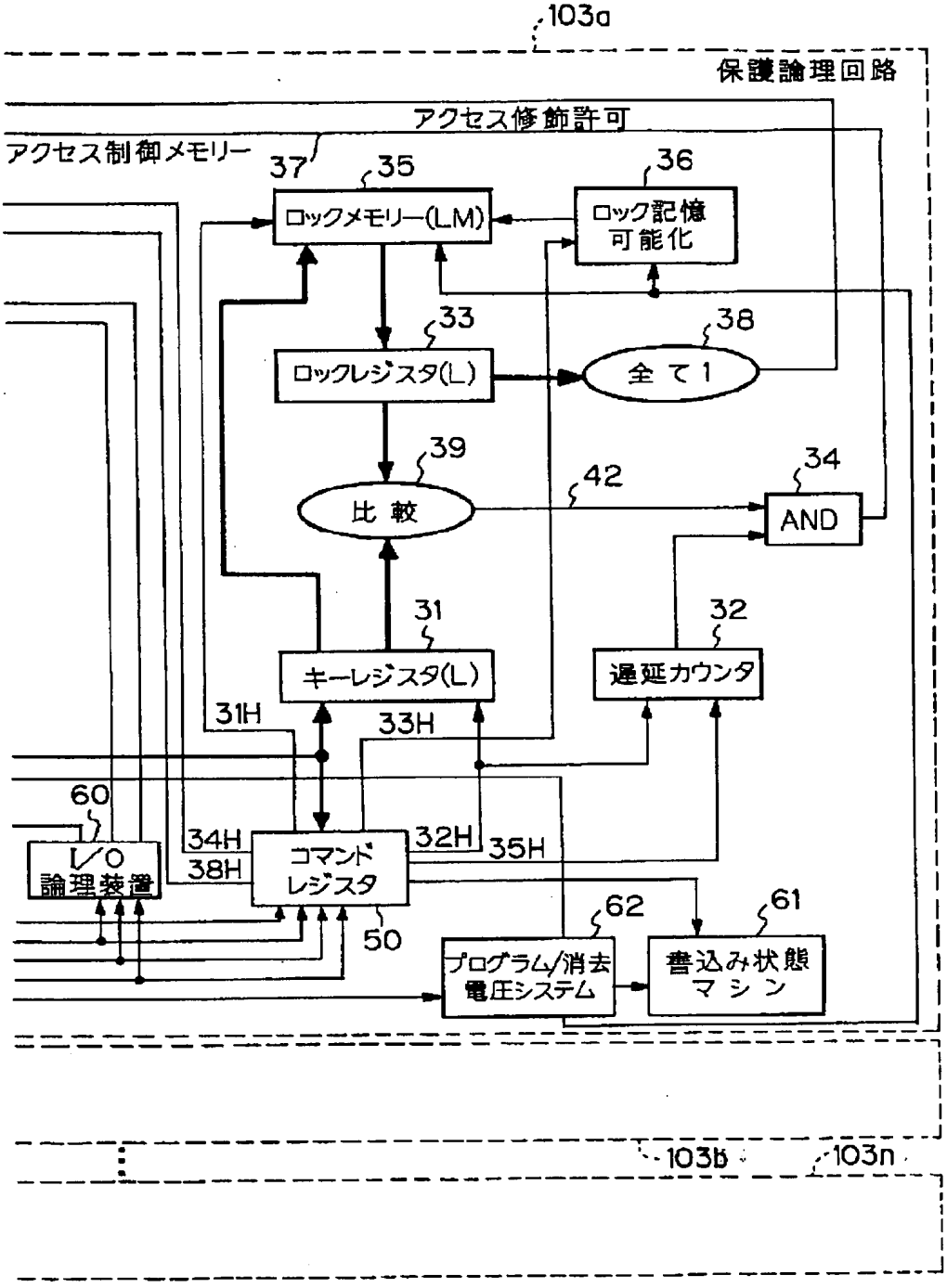
【図１】



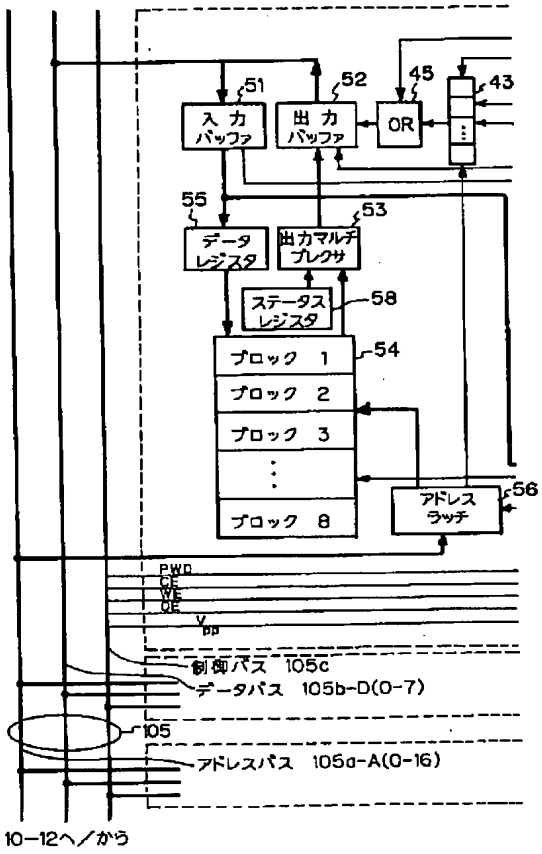
【図2】


105
105a
105b
105c
アドレス
データ
制御
10
アクセス制御プロセッサ
10-4
レジスタ RAM
10-6
プロセッサ
インターフェース
論理装置
10-12
10-2
Pin プロトコル
パスワード／PINs
インターバル・カウンタ
構成情報
(アプリケーション明細)
キー1 - フラッシュメモリー 103a
キー2 - フラッシュメモリー 103b
キーn - フラッシュメモリー 103n
プログラム
10-8
インターバル・タイマ
10-2a
10-2b
10-2c

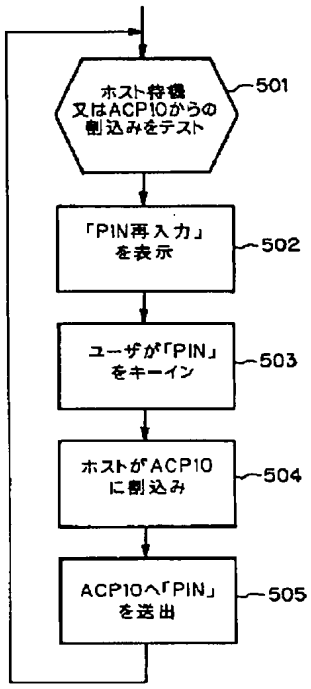
【図3】


103a
保護論理回路
アクセス修飾許可
アクセス制御メモリー
37
35
ロックメモリー(LM)
36
ロック記憶可能化
33
ロックレジスタ(L)
38
全て1
39
比較
42
34
AND
31
キーレジスタ(L)
32
遅延カウンタ
31H
33H
60
I/O論理装置
34H
38H
コマンドレジスタ
32H
35H
50
62
プログラム/消去電圧システム
61
書込み状態マシン
103b
103n

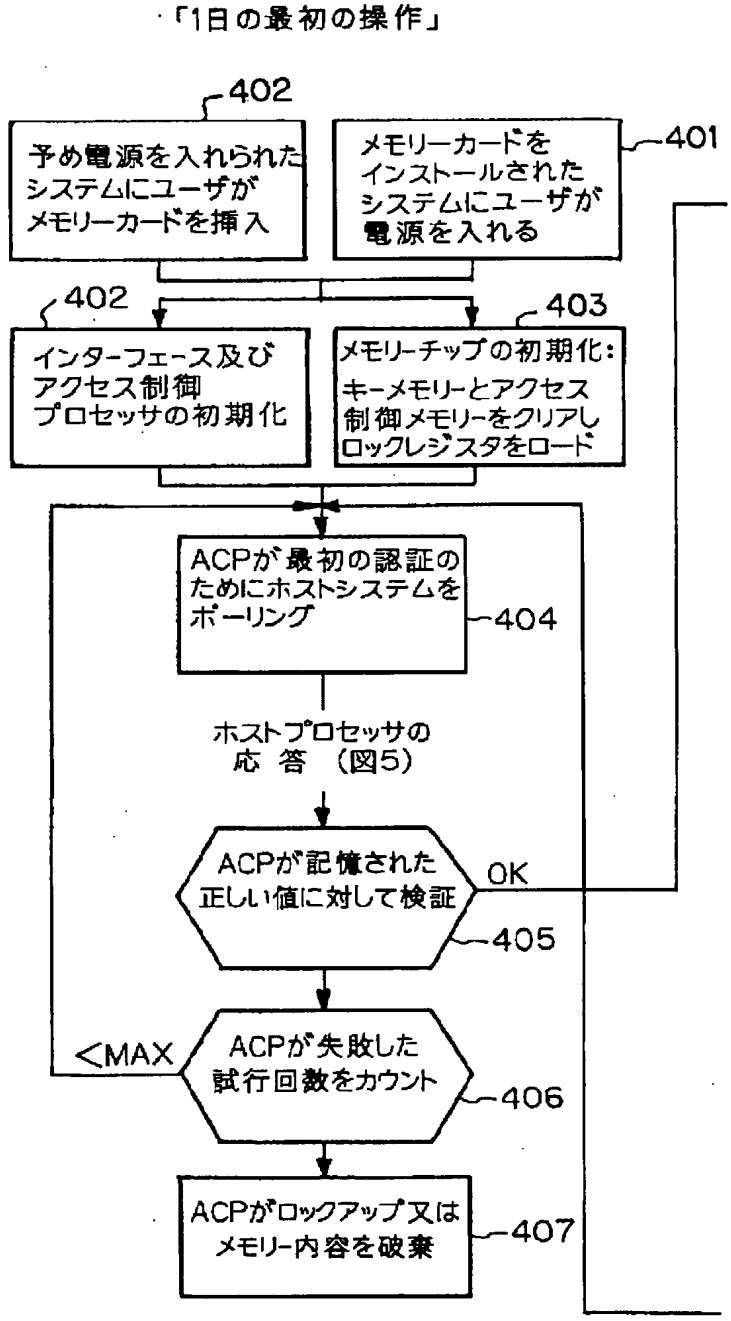
【図４】


51
52
45
43
入力バッファ
出力バッファ
OR
55
53
データレジスタ
出力マルチプレクサ
ステータスレジスタ
58
ブロック 1
ブロック 2
ブロック 3
ブロック 8
54
アドレスラッチ
56
PWD
CE
WE
OE
Vpp
制御バス 105c
データバス 105b-D(0-7)
105
アドレスバス 105a-A(0-16)
10-12へ／から

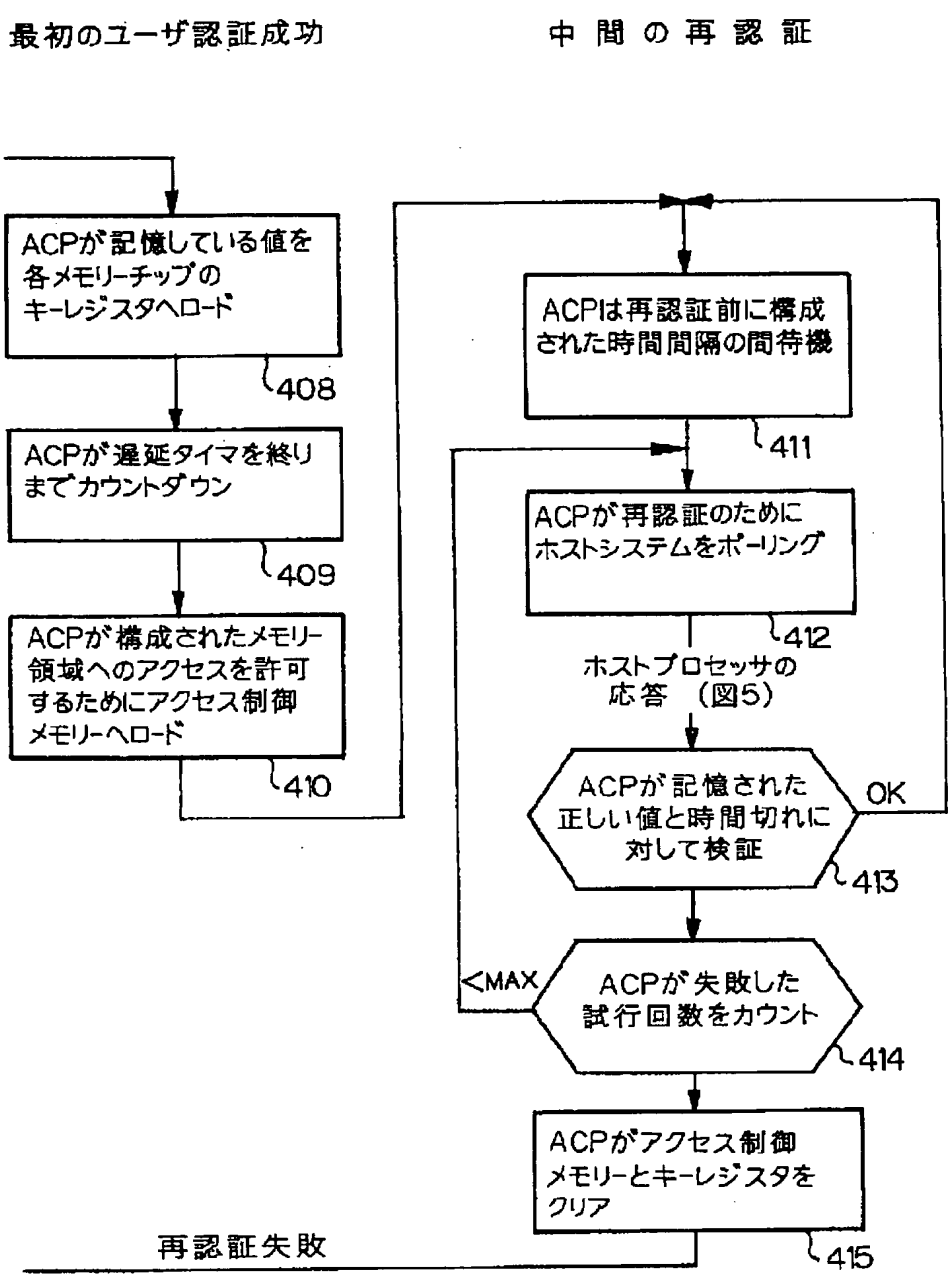
【図７】


ホスト待機
又はACP10からの
割込みをテスト
501
「PIN再入力」
を表示
502
ユーザが「PIN」
をキーイン
503
ホストがACP10
に割込み
504
ACP10へ「PIN」
を送出
505

【図5】


「1日の最初の操作」
402
予め電源を入れられたシステムにユーザがメモリーカードを挿入
メモリーカードをインストールされたシステムにユーザが電源を入れる
401
402
インターフェース及びアクセス制御プロセッサの初期化
403
メモリーチップの初期化：キーメモリーとアクセス制御メモリーをクリアしロックレジスタをロード
ACPが最初の認証のためにホストシステムをポーリング
404
ホストプロセッサの応答（図5）
ACPが記憶された正しい値に対して検証
OK
405
<MAX
ACPが失敗した試行回数をカウント
406
ACPがロックアップ又はメモリー内容を破棄
407

【図６】



フロントページの続き

(72)発明者　ピーター・ジェイ・ウィルソン
アメリカ合衆国テキサス州78641，リーンダー，フォレスト・トレイル　102

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成１３年１月１９日（２００１．１．１９）

【公開番号】特開平６－２０８５１５
【公開日】平成６年７月２６日（１９９４．７．２６）
【年通号数】公開特許公報６－２０８６
【出願番号】特願平５－２５６７８６
【国際特許分類第７版】
G06F 12/14 320
【ＦＩ】
G06F 12/14 320 A

【手続補正書】
【提出日】平成１１年６月２９日（１９９９．６．２９）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【請求項１】　ホストの携帯コンピュータと共に使用される機密保護メモリー・カードにおいて、
前記ホスト・コンピュータに対しおよびこれからアドレス、データおよび制御情報を送受するように接続されたマイクロプロセッサを設け、該マイクロプロセッサは、複数のキー値を含む情報と構成情報とを記憶するアドレス指定可能不揮発性メモリーを含み、
前記マイクロプロセッサに接続されて、アドレスとデータと前記カードにより行われるべきメモリー動作を定義する制御情報とを伝送する内部バスと、
前記マイクロプロセッサと共通に前記内部バスに接続されて、前記アドレスとデータと制御情報とを受取る少なくとも１つの不揮発性のアドレス指定可能メモリーとを設け、前記メモリーは、不揮発性記憶セクションと機密保護制御セクションとを含み、該記憶セクションは複数のブロックに構成されたメモリー・アレイを含み、各ブロックは複数のアドレス指定可能な場所と前記記憶動作を行う制御論理手段とを有し、前記機密保護制御セクションは前記内部バスと前記制御論理手段と前記メモリー・アレイとに接続され、前記機密保護制御セクションは、
前記ブロックと関連する少なくとも一つの前記キー値と構成情報を記憶する複数の不揮発性および揮発性記憶装置と、
前記制御論理手段と前記記憶装置とに接続されたアクセス制御論理手段とを含み、該アクセス制御論理手段は、前記マイクロプロセッサが予め定めた確認手順が前記ホスト・コンピュータにより行われて前記アクセス制御論理手段が前記構成情報に従って前記メモリー・アレイからの前記情報の読出しを許容することを可能にしたと判定した後のみ、前記構成情報により指定される如き前記メモリー・アレイの前記ブロックのアドレス指定されたものに記憶された情報の読出しを可能にすることを特徴とするメモリー・カード。
【請求項２】　前記マイクロプロセッサおよび前記不揮発性メモリーが個々の半導体チップ上に含まれることを特徴とする請求項１記載のメモリー・カード。
【請求項３】　前記カードが更に、該カードを前記ホスト・コンピュータに接続するインターフェース回路手段を含み、該インターフェース回路手段および前記マイクロプロセッサが同じ半導体チップ上に含まれることを特徴とする請求項１記載のメモリー・カード。
【請求項４】　前記不揮発性メモリー・カードおよび前記不揮発性記憶装置がフラッシュ・メモリーであることを特徴とする請求項１記載のメモリー・カード。
【請求項５】　前記不揮発性記憶装置の一方が、前記１つのキー値と対応するロック値を記憶するロック・メモリーであり、前記不揮発性装置の第２のものが前記ロック・メモリーに接続するロック記憶可能化要素であり、前記ロック・メモリーが最初に前記ロック値でロードされ、前記ロック記憶可能化要素が、前記マイクロプロセッサの制御下で前記ロック値の修正を禁止する状態へ切換えられることを特徴とする請求項１記載のメモリー・カード。
【請求項６】　前記ロック値の記憶および前記ロック記憶可能化要素の切換えが、前記メモリー・カードの初期の製造中に起生することを特徴とする請求項２記載のメモリー・カード。
【請求項７】　前記揮発性記憶装置の一方が、数において前記構成情報を記憶するための前記メモリー・アレイのブロック数と対応する複数の記憶域を持つアドレス指定可能なアクセス制御メモリーであり、該アクセス制御メモリーが前記内部バスと前記アクセス制御論理手段とに接続され、前記予め定めた確認手順が、前記アクセス

制御論理手段による前記アクセス制御メモリーの可能化を生じる前記ホスト・コンピュータにより最初に成功裏に行われたことを判定した後にのみ、前記アクセス制御メモリーが前記マイクロプロセッサの制御下でロードされることを特徴とする請求項５記載のメモリー・カード。

【請求項８】　前記ロック・メモリーにロードされた前記ロック値が全て１であり、前記機密保護制御セクションが更に、前記ロック・メモリーに接続された全て１の検出回路を含み、該検出回路が前記全て１のロック値に応答して、前記機密保護制御セクションを有効にバイパスする信号を生成して、前記不揮発性メモリーがあたかも前記機密保護制御セクションが含まれなかったかのように動作することを可能にすることを特徴とする請求項７記載のメモリー・カード。

【請求項９】　前記予め定めた確認手順の実施が、前記メモリー・カードが前記ホスト・コンピュータと通信するように最初に接続される時に初めて起生することを特徴とする請求項７記載のメモリー・カード。

【請求項１０】　前記アクセス制御メモリーが、前記ロック・メモリーから前記ロック値を受取るように接続されたロック・レジスタと、コンパレータ回路と、前記マイクロプロセッサにより前記キー・レジスタに送られるキー値を記憶するキー・レジスタと、予め定めた時間間隔を定義するカウントを記憶する遅延カウンタと、前記アクセス制御メモリーと前記コンパレータと前記遅延カウンタとに接続されたゲート手段とを含み、前記コンパレータ回路が、前記ロックおよびキー・レジスタと前記ゲート手段とに接続され、該ゲート手段が前記遅延カウンタに接続されて、前記遅延カウンタが前記予め定めた時間間隔の終りを信号した時前記ロック・レジスタにロードされる前記ロック・コード値間の同じ比較を信号する前記コンパレータ回路に応答してアクセス修正許容信号を生じ、前記アクセス修正許容信号が前記構成情報をロードするように前記アクセス制御メモリーを条件付ける信号を許容することを特徴とする請求項９記載のメモリー・カード。

【請求項１１】　前記制御論理手段が、各メモリー・チップの前記機密保護制御セクションの動作を制御する際に前記マイクロプロセッサにより使用される予め定めた指令セットに応答して指令信号を生じる回路を含むことを特徴とする請求項１０記載のメモリー・カード。

【請求項１２】　前記制御論理手段が、前記マイクロプロセッサにより生じる前記予め定めた指令セットの最初のものに応答して、前記ロック・コード値を前記ロック・メモリーにロードする第１の信号を生じ、該予め定めた指令の前記最初のものが前記カードの初期の製造中に生成されることを特徴とする請求項１１記載のメモリー・カード。

【請求項１３】　前記制御論理手段が、前記マイクロプロセッサにより生成された前記予め定めた指令セットの第２のものに応答して、前記ロック記憶可能化要素を、前記ロック・メモリーに記憶された前記ロック値に対する前記読出しまたは修正を禁止する予め定めた状態へ切換えるための第２の信号を生じることを特徴とする請求項１２記載のメモリー・カード。

【請求項１４】　前記制御論理手段が、前記マイクロプロセッサにより生じた前記予め定めた指令セットの第３のものに応答して、前記キー値の予め定めたもので前記予め定めたキー・レジスタをロードする第３の信号を生じ、前記予め定めた指令セットの前記第３のものが、前記予め定めた確認手順が成功裏に行われたことを前記マイクロプロセッサが判定した後にのみ、前記マイクロプロセッサにより生じることを特徴とする請求項１２記載のメモリー・カード。

【請求項１５】　前記制御論理手段により生じる前記第３の信号が、前記遅延カウンタを前記予め定めた時間間隔の開始を確立する予め定めたカウントに同時に強制し、前記制御論理手段が、前記マイクロプロセッサにより生じる前記予め定めた指令セットの第４のものの各々に応答して前記予め定めたカウントを１だけ減分し、前記遅延カウンタが、前記予め定めた指令セットの予め定めた数の前記第４のものの実行に続く前記時間間隔の前記終りを信号することを特徴とする請求項１４記載のメモリー・カード。

【請求項１６】　前記予め定めた制御論理手段が、前記マイクロプロセッサによる前記予め定めた指令セットの第５および第６の複数に応答して、情報の読出しが許容される前記ブロックのどれかを判定するため前記構成情報に従って前記アクセス制御メモリーにおける場所をセットしリセットするための第５および第６の信号を生じることを特徴とする請求項１１記載のメモリー・カード。

【請求項１７】　前記ホスト・コンピュータとの通信を確立するためホストの携帯コンピュータに組込み可能な機密保護メモリー・カードにおいて、

単一の半導体チップ上に含まれるマイクロプロセッサを設け、該マイクロプロセッサは、前記ホスト・コンピュータに対しかつこれからアドレスとデータと制御情報とを送受するよう接続され、該マイクロプロセッサは、

記憶域に対するユーザのアクセス可能性を定義する複数のキー値を含む情報と、前記記憶域に対するメモリー読出しアクセス可能性を定義するメモリー構成情報とを記憶するためのアドレス指定可能な不揮発性メモリーを含み、

アドレスとデータと前記カードにより行われるべき記憶動作を定義する制御情報とを伝送する内部バスと、

前記アドレスとデータと制御情報とを受取るため前記マイクロプロセッサと共通に前記内部バスに接続された少なくとも１つの不揮発性のアドレス指定可能なメモリー

・チップとを設け、該メモリー・チップは１つの記憶セクションと１つの機密保護セクションとを含み、該記憶セクションはデータ出力を有する不揮発性のメモリー・アレイを含んで各々が複数のアドレス指定可能な場所を有する複数のブロックに構成され、前記記憶動作を行うための制御論理手段を含み、前記機密保護セクションは、前記内部バスと前記制御論理手段と前記データ出力とに接続され、該機密保護セクションは、
前記内部バスに接続されて前記キー値数の１つと合致する予め定めたロック値を最初に受取りかつこれを恒久的に記憶する不揮発性ロック・メモリーと、
前記制御論理手段および前記ロック・メモリーと接続されて、前記予め定めたロック・コード値が前記マイクロプロセッサにより前記内部バスに与えられた前記キー値の選択された１つに識別可能に合致する時を検出すると同時に、可能化信号を生じるアクセス制御論理手段と、
前記読出し可能性を定義する前記記憶構成情報を記憶するための数において前記メモリー・アレイの前記ブロック数と対応する複数の場所を有するアドレス指定可能な揮発性アクセス制御メモリーとを含み、前記アクセス制御メモリーが、前記制御論理手段と前記メモリー・アレイのデータ出力と前記内部バスと前記アクセス制御論理手段とに接続され、該アクセス制御論理手段は、予め定めた確認手順が前記ホスト・コンピュータにより成功裏に行われ、かつ前記記憶のキー・コードの前記予め定めた１つを転送して、前記アクセス制御メモリーの構成情報により指定される如き前記データ出力に加えるための前記可能化信号を、前記アクセス制御論理手段をして前記データ出力に加えられる前記可能化信号を生じさせたことを前記マイクロプロセッサが判定した後にのみ、前記記憶構成情報により指定される如き前記メモリー・アレイの読出しを可能にすることを特徴とするメモリー・カード。

【請求項１８】　各々が複数のモードにおける動作能力を有するアドレス指定可能な場所のブロックに構成されたメモリー・アレイを含む複数の不揮発性メモリー・チップを含む機密保護メモリー・カードにおいて、
ロック値を記憶するロック・メモリーと、
第１および第２の指令と予め定めたキー値とを生成する制御手段と、
前記制御手段に接続されて、前記第１の指令に応答して前記予め定めたキー値を記憶するキー・レジスタと、
前記ロック・メモリーおよび前記キー・レジスタに接続され、前記ロック値および前記予め定めたキー値が等しい時は常に比較信号を生成するコンパレータと、
前記生成手段に接続され、かつ前記第１の指令に応答して前記カウンタを最大カウント値に設定し、かつ一連の連続する第２の指令に応答して前記遅延カウンタがゼロに減分された時ゼロ・カウント信号を生じる遅延カウンタと、
前記コンパレータおよび前記遅延カウンタに接続され、前記比較信号および前記ゼロ・カウント信号に応答してアクセス修正許容信号を生じる論理回路手段とを設け、
前記制御手段が、第３の指令と、前記第１のブロックおよび以降のブロックをそれぞれ識別する第１のアドレス信号と以降のアドレス信号とを生じ、
前記論理手段と前記制御手段とに接続されたアクセス制御メモリー手段を設け、該アクセス制御メモリーは、前記アクセス記憶可能化信号と前記アドレス信号と前記第３の指令とに応答して、前記ブロックおよび前記以降のブロックの内の一つが読出しのため可能状態にされる時を指定する表示を記憶することを特徴とするメモリー・カード。

【請求項１９】　前記メモリー・カードが不当なホスト・コンピュータに配置される時、前記予め定めた値および最大値が、前記不揮発性メモリーに記憶された前記情報に対する容易なアクセスを阻止するように充分に大きく選定されることを特徴とする請求項１８記載のシステム。

【請求項２０】　前記制御手段が、第１のユーザの確認動作を成功裏に行ったと同時に、前記第１、第２および第３の指令を生じる前記メモリーに接続するマイクロプロセッサを含むことを特徴とする請求項１８記載のカード。

【請求項２１】　前記第１の指令がロード・キー指令であり、前記第２の指令が減分指令であり、前記第３の指令が読出し許容ブロック指令であることを特徴とする請求項２０記載のカード。

【請求項２２】　前記メモリーが更に、前記カードを正常な記憶動作を行うように条件付ける予め定めた指令セットを復号する指令制御手段を含み、前記指令制御手段が、前記第１、第２および第３の指令を含む別の指令セットを復号して前記メモリーに記憶された情報に対する機密保護を行う手段を含むことを特徴とする請求項１８記載のカード。

【請求項２３】　各々がアドレス指定可能な場所に構成されたメモリー・アレイを含む複数の不揮発性メモリー・チップと、記憶動作を行う指令信号を生じる制御論理回路を含むホスト・コンピュータに組込み可能な機密保護メモリー・カードを構成する方法において、
（ａ）組込まれた時前記ホスト・コンピュータと通信するように接続される前記カードにマイクロプロセッサを組込み、該マイクロプロセッサは、記憶域に対するユーザのアクセス可能性を定義する複数のキー値を含む情報と、前記記憶域に対するアクセス可能性を定義するメモリー構成情報とを記憶するためのアドレス指定可能な不揮発性メモリーを含み、
（ｂ）機密保護論理回路を各不揮発性メモリー・チップに組込み、該機密保護論理回路が、予め定めたロック値を記憶する不揮発性ロック・メモリーと、該ロック・メ

モリーと接続されたアクセス制御論理手段と、前記構成情報に従ってアクセス可能性のビット情報を記憶する前記ブロック数と対応する複数の場所を有するアドレス指定可能な揮発性アクセス制御メモリーとを含み、
（ｃ）前記マイクロプロセッサを各メモリー・チップに組込み、アドレスとデータと制御情報とを前記各メモリー・チップへ転送し、
（ｄ）複数の指令に応答して前記機密保護論理回路を動作させるよう前記制御論理回路を修正し、
（ｅ）前記ホスト・コンピュータと共に前記マイクロプロセッサによる初期の予め確立されたユーザ確認動作を実施し、
（ｆ）ステップ（ｅ）における前記確認動作が成功裏に行われた時にのみ、前記各チップに対して前記複数の指令の特定のものを転送する前記マイクロプロセッサにより前記機密保護論理回路を可能状態にして、前記ブロックの異なるものに記憶された前記情報を前記アクセス制御メモリーに記憶された前記アクセス可能性ビット情報に従って読出すことを許容するステップを含むことを特徴とする方法。
【請求項２４】　前記マイクロプロセッサの不揮発性メモリーが複数のセクションを有し、ステップ（ａ）が更に、前記キー値に対する乱数を生成して該キー値を前記セクション数の最初のものにロードするステップを含むことを特徴とする請求項２３記載の方法。
【請求項２５】　前記マイクロプロセッサが更に、前記マイクロプロセッサの不揮発性メモリーに接続されたインターバル・カウンタを含み、ステップ（ａ）が更に、ユーザが選択した時間間隔を生成して該ユーザ選択時間間隔値と対応する値を前記インターバル・カウンタへロードするステップを含み、更に
（ｇ）前記ユーザ選択時間間隔でステップ（ｅ）の前記ユーザ確認動作を周期的に開始し、
（ｈ）ステップ（ｂ）の前記確認動作が成功裏に行われる限り、前記ブロックに記憶された前記情報が前記アクセス可能性ビット情報に従って読出されることを許容し続けるステップを含むことを特徴とする請求項２４記載の方法。
【請求項２６】　各々がアドレス指定可能な場所のブロックに構成されたメモリー・アレイを含む多数の情報を記憶するための複数の不揮発性メモリー・チップと、記憶動作を行うための指令信号を生成する制御論理回路とを含む機密保護メモリー・カードを構成する方法において、
（ａ）記憶域に対するユーザのアクセス可能性を定義する多数のキー値を含む情報と、前記記憶域に対するアクセス可能性を定義するメモリー構成情報とを記憶するためのアドレス指定可能な不揮発性メモリーを含むマイクロプロセッサを前記カードに組込み、
（ｂ）予め定めたロック値を記憶する不揮発性ロック・メモリーと、該ロック・メモリーに接続されたアクセス制御論理手段と、前記構成情報に従ってユーザのアクセス可能性ビット情報を記憶する前記多数のブロックと数において対応する複数の場所を有するアドレス指定可能な揮発性アクセス制御メモリーとを含む機密保護論理回路を各不揮発性メモリー・チップに組込み、
（ｃ）アドレスとデータと制御情報とを前記各メモリー・チップへ転送するため前記マイクロプロセッサを各メモリー・チップに相互に接続し、
（ｄ）前記制御論理回路により通常与えられる１組の指令に対する拡張として前記機密保護論理回路を動作させる複数の指令を組込むように前記制御論理回路を修正することにより、前記機密保護論理回路が、前記多数のチップが前記メモリー・カードから取外される場合でも、前記チップに含まれる前記情報が不当な方法で読出されることを防護するステップを含むことを特徴とする方法。
【請求項２７】　不揮発性記憶セクションと機密保護制御セクションとを含む不揮発性メモリー・チップ（１０３ａ）であって、前記記憶セクションは、一方では、夫々複数のアドレス指定可能な場所を有する幾つかのブロックに構成されたメモリー・アレイ（５４）を、他方では、記憶動作を行う制御論理手段（５０）を含み、前記機密保護制御セクションは、前記制御論理手段及び前記メモリー・アレイに接続されており、該機密保護制御セクションが、
前記ブロックと関連する少なくとも１つのキー値と構成情報を記憶する複数の不揮発性記憶装置（３１、３５）及び揮発性記憶装置（３３、４３）と、
前記制御論理手段（５０）と前記複数の記憶装置に接続されたアクセス制御論理手段（３２、３４、３９）とを含み、該アクセス制御論理手段は、前記メモリー・チップ（１０３ａ）が外部のマイクロプロセッサ（１０）から予め定めた認証手順がユーザによって実行されたことを示す信号を受け取った後にのみ、前記構成情報によって特定された前記メモリー・アレイ（５４）のアドレス指定された前記ブロックの内の１つに記憶された情報の読み出しを可能にし、前記アクセス制御論理手段（３２、３４、３９）が前記構成情報に従って前記メモリー・アレイ（５４）から前記情報の読み出しを許すことを可能にする、
ことを特徴とするメモリー・チップ。